配置 ASA 设备

本章涵盖以下部分：

- 更新 ASA 连接凭证， 第 2 页
- ASA 接口配置， 第 3 页
- ASA 系统设置策略 ， 第 14 页
- ASA 路由， 第 24 页
- 安全策略管理， 第 27 页
- 管理传统 ASA 访问策略， 第 27 页
- ASA 策略（扩展访问列表）, on page 37
- 配置 ASA 全局访问策略， 第 38 页
- 命中率, on page 40
- 导出网络策略规则, on page 41
- 将 ASA 策略更改应用于设备， 第 41 页
- ASA 策略中的安全组标记， 第 42 页
- 影子规则， 第 42 页
- 网络地址转换， 第 44 页
- NAT 规则的处理顺序, on page 45
- 网络地址转换向导, on page 46
- NAT 常见使用案例， 第 47 页
- 在 CDO 中管理虚拟专用网络管理， 第 56 页
- ASA 模板, on page 123
- API 令牌， 第 125 页
- 将 ASA 配置迁移到 FDM 管理 设备模板, on page 126
- 管理 ASA 证书， 第 126 页
- ASA 文件管理, on page 134
- 管理 ASA 高可用性， 第 137 页
- 在 ASA 上配置 DNS, on page 138
- CDO 命令行界面, on page 139
- 批量命令行接口, on page 141
- 命令行界面宏, on page 144

- 使用 CDO CLI 配置 ASA， 第 148 页
- 使用 CDO 来比较 ASA 配置, on page 149
- ASA 批量 CLI 使用案例, on page 149
- ASA 命令行接口文档, on page 151
- 导出 CDO CLI 命令结果, on page 152
- 恢复 ASA 配置, on page 154
- 管理 ASA 和 Cisco IOS 设备配置文件, on page 156
- 读取、丢弃、检查和部署更改， 第 158 页
- 读取所有设备配置, on page 159
- 将 ASA 的配置更改读取到 CDO， 第 160 页
- 预览和部署所有设备的配置更改， 第 160 页
- 将配置更改从 CDO 部署到 ASA， 第 161 页
- 批量部署设备配置, on page 165
- 已计划的自动部署, on page 166
- 检查配置更改, on page 168
- 放弃更改, on page 169
- 设备上的带外更改, on page 169
- 同步 Defense Orchestrator 和设备之间的配置， 第 170 页
- 冲突检测, on page 170
- 自动接受设备的带外更改, on page 171
- 解决配置冲突, on page 172
- 安排设备更改轮询, on page 173

更新 ASA 连接凭证

在载入 ASA 的过程中，您输入了 CDO 必须用于连接到设备的用户名和密码。如果这些凭证在设备上发生更改，请使用更新凭证设备操作在 CDO 上更新这些凭证。此功能允许您更新 CDO 上的凭证，而无需重新载入设备。切换到的用户名和密码组合必须已存在于该用户的 ASA 或身份验证、授权和审计 (AAA) 服务器上。此过程仅影响 Cisco Defense Orchestrator 数据库；使用更新凭证功能时，不会对 ASA 配置进行任何更改。

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡，然后点击 **ASA**。

步骤 3 选择要更新其连接凭证的 ASA。您可以一次更新一个或多个 ASA 上的凭证。

步骤 4 在**设备操作 (Device Actions)** 窗格中，点击**更新凭证 (Update Credentials)**。

步骤 5 选择用于将 ASA 连接到 CDO 的云连接器或安全设备连接器 (SDC)。

步骤 6 输入要用于连接到 ASA 的新用户名和密码。

步骤 7 凭证更改后，CDO 会同步设备。

注释　如果 CDO 无法同步设备，CDO 中的连接状态可能会显示“无效凭证”(Invalid Credentials)。如果是这种情况，您可能尝试使用无效的用户名和密码组合。请确保要使用的凭证已存储在 ASA 或 AAA 服务器上，然后重试。

将 ASA 从一个 SDC 移至另一个 SDC

CDO 支持每个租户使用多个 SDC。在单个 CDO 租户上使用多个 SDC您可以使用以下程序将受管 ASA 从一个 SDC 移至另一个 SDC：

步骤 1 在 CDO 菜单栏中，点击**清单 (Inventory)**。

步骤 2 选择要移动到其他 SDC 的 ASA。

步骤 3 在“设备操作”(Device Actions) 窗格中，点击**更新凭证 (Update Credentials)**。

步骤 4 点击 Secure Device Connector 按钮，然后选择要将设备移动到的 SDC。

步骤 5 输入用于载入 ASA 的管理员用户名和密码，然后点击更新。您不必将这些更改部署到设备。

ASA 接口配置

Cisco Defense Orchestrator (CDO) 通过提供无需使用命令行界面的用户友好界面来简化 ASA 接口配置。您可以完全控制 ASA 的物理接口、子接口和 EtherChannel 的配置。此外，您还可以查看在基于路由的站点间 VPN 期间创建的虚拟隧道接口，但它们是只读的。您可以使用 CDO 来配置和编辑 ASA 设备上的数据接口或管理/诊断接口。

将电缆（以物理方式或虚拟方式）连接到接口接头时，您需要配置该接口。至少需要命名并启用该接口，流量才会通过该接口。如果该接口是网桥组的成员，则只用为接口命名。如果接口是桥接虚拟接口 (BVI)，则需要为 BVI 分配一个 IP 地址。如果要在特定端口上创建 VLAN 子接口（而非单一物理接口），通常要在该子接口（而不是物理接口）上配置 IP 地址。通过 VLAN 子接口，可将一个物理接口划分成多个标记有不同 VLAN ID 的逻辑接口。

接口列表将显示可用的接口及其名称、地址和状态。您可以通过选择接口行并点击“操作”(Actions) 窗格中的**编辑 (Edit)** 来更改接口的状态（打开或关闭）或编辑接口。列表将基于您的配置显示接口特征。展开接口行以查看子接口或桥接组成员。

管理接口

可以通过连接至以下接口来管理 ASA：

- 任何直通流量接口
- 专用的管理插槽/端口接口（如果适用于所用的型号）

使用 MTU 设置

MTU 会指定设备可在给定以太网接口上传输的最大帧负载大小。MTU 值是没有以太网报头、VLAN 标记或其他系统开销情况下的帧大小。例如，将 MTU 设置为 1500 时，预期帧大小为 1518 字节（含报头）或 1522 字节（使用 VLAN）。请勿为容纳这些报头而将 MTU 的值设得过高。

虚拟隧道接口 (VTI) 的只读支持

在两台 ASA 设备之间配置基于路由的站点间 VPN 隧道会在设备之间创建虚拟隧道接口 (VTI)。已配置 VTI 隧道的设备可以载入 CDO，CDO 会在 **ASA 接口 (ASA Interfaces)** 页面上发现并列出这些隧道，但不支持对其进行管理

配置 ASA 物理接口

步骤 1 在 CDO 导航窗格，点击**清单 (Inventory)**。

步骤 2 点击 **ASA** 选项卡。

步骤 3 选择您要修改的设备，然后在右侧的**管理 (Management)** 窗格中点击**接口 (Interfaces)**。

步骤 4 点击要配置的物理接口，然后点击 **Edit**。

系统将显示**编辑物理接口 (Editing Physical Interface)** 对话框。

步骤 5 在**逻辑名称 (Logical Name)** 字段中，输入接口名称。

步骤 6 继续执行以下程序之一：

- 如果要为物理接口分配 IPv4 地址，请为 ASA 物理接口配置 IPv4 地址。
- 为 ASA 物理接口配置 IPv6 地址，第 5 页 如果打算为该接口分配 IPv6 地址。
- 配置高级 ASA 物理接口选项。高级设置的默认值适用于大多数网络。只有在需要解决网络问题时，再进行编辑。
- 如果您保存了接口并且不想继续使用高级接口选项，请继续启用 ASA 物理接口。

为 ASA 物理接口配置 IPv4 地址

步骤 1 在**编辑物理接口 (Edit Physical Interface)** 对话框中，在 **IPv4 地址 (IPv4 Address)** 选项卡中配置以下内容：

- **类型 (Type)**：您可以为接口使用静态 IP 寻址或 DHCP。

  静态 (Static) - 如果希望分配固定的地址，请选择此选项。

  - **IP 地址和子网掩码 (IP Address and Subnet Mask)**：对于连接到接口的网络，键入接口的 IP 地址和子网掩码。

- **备用 IP 地址 (Standby IP Address)**：如果您配置了高可用性，并为高可用性监控此接口，请在同一子网上配置备用 IP 地址。备用设备上的此接口使用备用地址。

  为每个接口设置一个备用 IP 地址。虽然建议指定备用 IP 地址，但它并不是必需的。如果没有备用 IP 地址，则主用设备无法执行用于检查备用接口运行状态的网络测试；它只能跟踪链路状态。

DHCP：如果应从网络中的 DHCP 服务器获取地址，请选择此选项。

您可以选中**获取默认路由 (Obtain Default Route)** 复选框以便从 DHCP 服务器获取默认路由。您通常都要选中此选项。

步骤 2 完成后点击**保存 (Save)**，或者继续执行其中一个程序。

- 为 ASA 物理接口配置 IPv6 地址，第 5 页 如果打算为该接口分配 IPv6 地址。
- 配置高级 ASA 物理接口选项。高级设置的默认值适用于大多数网络。只有在需要解决网络问题时，再进行编辑。
- 如果您保存了接口并且不想继续使用高级接口选项，请继续启用 ASA 物理接口。

为 ASA 物理接口配置 IPv6 地址

步骤 1 在**编辑物理接口 (Editing Physical Interface)** 对话框中，点击 **IPv6 地址 (IPv6 Address)** 选项卡。

步骤 2 进行以下配置：

- **状态 (State)** - 在您未配置全局地址时，要启用 IPv6 处理并自动配置本地链路地址，请点击**状态 (State)** 滑块将其启用。本地链路地址基于接口的 MAC 地址（修改的 EUI-64 格式）生成。

  注释 禁用 IPv6 不会禁用接口上使用显式 IPv6 地址配置或启用自动配置的 IPv6 处理。

- **地址自动配置**：

  选中此选项可自动配置地址。只有设备所在链路中的路由器配置为提供 IPv6 服务（包括通告 IPv6 全局前缀以用于该链路），IPv6 无状态自动配置才会生成全局 IPv6 地址。如果该链路中的 IPv6 路由服务不可用，则只能获得本地链路 IPv6 地址，无法访问设备直接的网络链路之外的服务。本地链路地址以修改的 EUI-64 接口 ID 为基础。

  虽然 RFC 4862 规定为无状态自动配置所配置的主机不发送路由器通告消息，但设备在这种情况下确实会发送路由器通告消息。选择**抑制 RA** 可抑制消息，遵从 RFC 要求。

- **抑制 RA (Suppress RA)**：如果要抑制路由器通告，请选中此复选框。设备可以参与路由器通告，以便邻居设备可以动态获悉默认路由器地址。默认情况下，每个配置 IPv6 的接口定期发送路由器通告消息（ICMPv6 类型 134）。

  也会发送路由器通告，以响应路由器请求消息（ICMPv6 类型 133）。路由器请求消息由主机在系统启动时发送，以便主机可以立即自动配置，而无需等待下一条预定路由器通告消息。

  对于不希望设备提供 IPv6 前缀的任何接口（例如外部接口），您可能希望抑制接口上的这些消息。

- **DAD 尝试 (DAD Attempts)**：接口执行重复地址检测 (DAD) 的频率，介于 0 - 600 之间。默认值为 1。在无状态自动配置过程中，DAD 会验证新单播 IPv6 地址的唯一性，再将地址分配给接口。如果重复地址是接口的链路本地地址，则在接口上禁用 IPv6 数据包处理。如果重复地址是全局地址，则将不使用该地址。接口将使用邻居的询求消息来执行重复地址检测。将该值设置为 0 可禁用重复地址检测 (DAD) 流程。
- **本地链路地址 (Link-Local Address)**：如果要仅将地址用作链路本地地址，请在链路本地地址字段中输入该地址。本地链路地址在本地网络之外无法访问。在网桥组接口上无法配置本地链路地址。

  注释 链路本地地址应以 FE8、FE9、FEA 或 FEB 开头，例如 fe80::20d:88ff:feee:6a82。请注意，我们建议根据修改的 EUI-64 格式自动分配链路本地地址。例如，如果其他设备强制使用修改的 EUI-64 格式，则手动分配的链路本地地址可能导致丢弃数据包。

- **备用链路本地地址 (Standby Link-Local Address)**：如果接口连接高可用性设备，请配置此地址。输入此接口所连接的另一台设备上的接口本地链路地址。
- **静态地址/前缀 (Static Address/Prefix)**：如果不使用无状态自动配置，请输入完整的静态全局 IPv6 地址和网络前缀。例如，2001:0DB8::BA98:0:3210/48。您可以添加另一个静态地址。
- **备用 IP 地址 (Standby IP Address)**： 如果您配置了高可用性，并为高可用性监控此接口，请在同一子网上配置备用 IPv6 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。

步骤 3 完成后点击**保存 (Save)**，或者继续执行其中一个程序。

- 配置高级 ASA 物理接口选项。高级设置的默认值适用于大多数网络。只有在需要解决网络问题时，再进行编辑。
- 如果您保存了接口并且不想继续使用高级接口选项，请继续启用 ASA 物理接口。

配置高级 ASA 物理接口选项

高级接口选项的默认设置适用于大多数网络。只有在需要解决网络问题时，再配置它们。

以下步骤程序假定已定义接口。另外，您还可以在初始编辑或创建接口时编辑这些设置。

此程序及其中的所有步骤都是可选的。

步骤 1 在**编辑物理接口 (Editing Physical Interface)** 对话框中，点击**高级 (Advanced)** 选项卡。

步骤 2 配置以下高级设置：

- **HA 监控 (HA Monitoring)**：启用后，可在当 HA 对决定是否在高可用性配置中故障转移到对等设备时考虑接口的运行状况。如果不配置高可用性，可忽略此选项。如果不配置接口的名称，也可以忽略此选项。
- **仅管理 (Management Only)**：启用后，可进行数据接口管理。

  仅管理接口不允许直通流量，所以将数据接口设置为**仅管理 (Management Only)** 接口的价值微乎其微。不能更改管理/诊断接口的此项设置，它们始终为仅管理。

- **MTU**：默认 MTU 为 1500 字节。您可以指定 64 - 9198 之间的值。如果通常在网络中使用巨帧，请设置一个较大的值。
- **复用和速度 (Mbps) (Duplex and Speed [Mbps])**：默认设置为该接口与线路另一端的接口协商最佳复用和速度，但如有必要，您可以强制实施特定的复用或速度。所列的选项仅为接口支持的设置。在网络模块上设置这些选项之前，请阅读接口配置限制。
  - **复用 (Duplex)** - 选择“自动”(Auto)、“半”(Half) 或“全”(Full)。当接口支持时，自动为默认值。
  - **速度 (Speed)** - 选择自动可使接口协商速度（默认值）或选取特定速度：10 Mbps、100 Mbps、1000 Mbps、10000 Mbps。此外，您还可以选择以下特殊选项：
- **DAD 尝试 (DAD Attempts)**：接口执行重复地址检测 (DAD) 的频率，介于 0 - 600 之间。默认值为 1。在无状态自动配置过程中，DAD 会验证新单播 IPv6 地址的唯一性，再将地址分配给接口。如果重复地址是接口的链路本地地址，则在接口上禁用 IPv6 数据包处理。如果重复地址是全局地址，则将不使用该地址。接口将使用邻居的询求消息来执行重复地址检测。将该值设置为 0 可禁用重复地址检测 (DAD) 流程。
- **MAC 地址 (MAC Address)**：采用 H.H.H 格式的介质访问控制，其中 H 是 16 位十六进制数字。例如，您可以将 MAC 地址 00-0C-F1-42-4C-DE 输入为 000C.F142.4CDE。MAC 地址不能设置组播位，即左起第二个十六进制数字不能是奇数。
- **备用 MAC 地址 (Standby MAC Address)**：用于高可用性。如果主用设备发生故障切换，备用设备变为主用设备，则新的主用设备开始使用主用 MAC 地址，以最大限度地减少网络中断，而原来的主用设备使用备用地址。

步骤 3 如果您保存了接口并且不想继续使用高级接口选项，请继续启用 ASA 物理接口。

步骤 4 点击**保存 (Save)**。

启用 ASA 物理接口

步骤 1 选择要启用的物理接口。

步骤 2 移动与接口逻辑名称关联的窗口右上角的**状态 (State)** 滑块。

步骤 3 预览和部署所有设备的配置更改所做的更改。

添加 ASA VLAN 子接口

通过 VLAN 子接口，可将一个物理接口划分成多个标记有不同 VLAN ID 的逻辑接口。带有一个或多个 VLAN 子接口的接口将自动配置为 802.1Q 中继。由于 VLAN 允许您在特定物理接口上将流量分开，所以您可以增加网络中可用的接口数量，而无需增加物理接口或设备。

如果您将物理接口连接到交换机的中继端口，请创建子接口。为交换机中继端口上显示的每个VLAN创建子接口。如果您将物理接口连接到交换机的接入端口，创建子接口将没有意义。

- 配置 ASA VLAN 子接口

为 ASA 子接口配置 IPv4 地址，第 8 页
- 为 ASA 子接口配置 IPv6 地址，第 9 页
- 配置高级 ASA 子接口选项，第 10 页
- 启用子接口，第 11 页

配置 ASA VLAN 子接口

步骤 1 在 CDO 导航窗格，点击**清单 (Inventory)**。

步骤 2 点击 **ASA** 选项卡。

步骤 3 选择您要修改的设备，然后在右侧的**管理 (Management)** 窗格中点击**接口 (Interfaces)**。

步骤 4 您可以使用以下方法之一来添加子接口：

- 选择  > **子接口 (Subinterface)**
- 点击要配置的物理接口，然后在右侧的**操作 (Actions)** 窗格中，点击**新建子接口 (New Subinterface)**。

步骤 5 在 **VLAN ID** 字段中，输入介于 1 和 4094 之间的 VLAN ID。

某些 VLAN ID 可能是连接的交换机中的保留 VLAN ID，因此请查看交换机文档以了解详细信息。对于多情景模式，您只能在系统配置中设置 VLAN。

步骤 6 在**子接口 ID (Subinterface ID)** 字段中，输入子接口 ID（介于 1 到 4294967293 之间的整数）。

允许的子接口数因平台而异。此 ID 一旦设置便不可更改。

步骤 7 继续执行以下程序之一：

- 如果要向此接口分配 IPv4 地址，请为 ASA 子接口配置 IPv4 地址。
- 如果要向此接口分配 IPv6 地址，请为 ASA 子接口配置 IPv6 地址。
- 配置高级 ASA 子接口选项。高级设置的默认值适用于大多数网络。只有在需要解决网络问题时，再进行编辑。
- 如果您保存了子接口，并且不想继续使用高级子接口选项，请继续启用子接口。

为 ASA 子接口配置 IPv4 地址

步骤 1 在**创建子接口 (Creating Subinterface)** 对话框中，在 **IPv4 地址 (IPv4 Address)** 选项卡中配置以下内容：

- **类型 (Type)**：您可以为接口使用静态 IP 寻址或 DHCP。

  静态 (Static) - 如果希望分配固定的地址，请选择此选项。

- **IP 地址和子网掩码 (IP Address and Subnet Mask)**：对于连接到接口的网络，键入接口的 IP 地址和子网掩码。
- **备用 IP 地址 (Standby IP Address)**：如果您配置了高可用性，并为高可用性监控此接口，请在同一子网上配置备用 IP 地址。备用设备上的此接口使用备用地址。

  为每个接口设置一个备用 IP 地址。虽然建议指定备用 IP 地址，但它并不是必需的。如果没有备用 IP 地址，则主用设备无法执行用于检查备用接口运行状态的网络测试；它只能跟踪链路状态。

DHCP：如果应从网络中的 DHCP 服务器获取地址，请选择此选项。

您可以选中**获取默认路由 (Obtain Default Route)** 复选框以便从 DHCP 服务器获取默认路由。您通常都要选中此选项。

步骤 2 完成后点击**保存 (Save)**，或者继续执行其中一个程序。

- 如果要向此接口分配 IPv6 地址，请为 ASA 子接口配置 IPv6 地址。
- 配置高级 ASA 子接口选项。高级设置的默认值适用于大多数网络。只有在需要解决网络问题时，再进行编辑。
- 如果您保存了子接口，并且不想继续使用高级子接口选项，请继续启用 ASA 物理接口。

为 ASA 子接口配置 IPv6 地址

步骤 1 在**创建子接口 (Creating Subinterface)** 对话框中，点击**IPv6 地址 (IPv6 Address)** 选项卡。

步骤 2 进行以下配置：

- **状态 (State)** - 在您未配置全局地址时，要启用 IPv6 处理并自动配置本地链路地址，请点击**状态 (State)** 滑块将其启用。本地链路地址基于接口的 MAC 地址（修改的 EUI-64 格式）生成。

  注释 禁用 IPv6 不会禁用接口上使用显式 IPv6 地址配置或启用自动配置的 IPv6 处理。

- **地址自动配置**：

  选中此选项可自动配置地址。只有设备所在链路中的路由器配置为提供 IPv6 服务（包括通告 IPv6 全局前缀以用于该链路），IPv6 无状态自动配置才会生成全局 IPv6 地址。如果该链路中的 IPv6 路由服务不可用，则只能获得本地链路 IPv6 地址，无法访问设备直接的网络链路之外的服务。本地链路地址以修改的 EUI-64 接口 ID 为基础。

  虽然 RFC 4862 规定为无状态自动配置所配置的主机不发送路由器通告消息，但设备在这种情况下确实会发送路由器通告消息。选择**抑制 RA** 可抑制消息，遵从 RFC 要求。

- **抑制 RA (Suppress RA)**：如果要抑制路由器通告，请选中此复选框。设备可以参与路由器通告，以便邻居设备可以动态获悉默认路由器地址。默认情况下，每个配置 IPv6 的接口定期发送路由器通告消息（ICMPv6 类型 134）。

也会发送路由器通告，以响应路由器请求消息（ICMPv6 类型 133）。路由器请求消息由主机在系统启动时发送，以便主机可以立即自动配置，而无需等待下一条预定路由器通告消息。

对于不希望设备提供 IPv6 前缀的任何接口（例如外部接口），您可能希望抑制接口上的这些消息。

- **DAD 尝试** - 接口执行重复地址检测 (DAD) 的频率，介于 0 - 600 之间。默认值为 1。在无状态自动配置过程中，DAD 会验证新单播 IPv6 地址的唯一性，再将地址分配给接口。如果重复地址是接口的链路本地地址，则在接口上禁用 IPv6 数据包处理。如果重复地址是全局地址，则将不使用该地址。接口将使用邻居的询求消息来执行重复地址检测。将该值设置为 0 可禁用重复地址检测 (DAD) 流程。
- **本地链路地址 (Link-Local Address)**：如果要仅将地址用作链路本地地址，请在链路本地地址字段中输入该地址。本地链路地址在本地网络之外无法访问。在网桥组接口上无法配置本地链路地址。

  注释 链路本地地址应以 FE8、FE9、FEA 或 FEB 开头，例如 fe80::20d:88ff:feee:6a82。请注意，我们建议根据修改的 EUI-64 格式自动分配链路本地地址。例如，如果其他设备强制使用修改的 EUI-64 格式，则手动分配的链路本地地址可能导致丢弃数据包。

- **备用链路本地地址 (Standby Link-Local Address)**：如果接口连接高可用性设备，请配置此地址。输入此接口所连接的另一台设备上的接口本地链路地址。
- **静态地址/前缀 (Static Address/Prefix)**：如果不使用无状态自动配置，请输入完整的静态全局 IPv6 地址和网络前缀。例如，2001:0DB8::BA98:0:3210/48。您可以添加另一个静态地址。
- **备用 IP 地址 (Standby IP Address)**：如果您配置了高可用性，并为高可用性监控此接口，请在同一子网上配置备用 IPv6 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。

步骤 3 完成后点击**保存 (Save)**，或者继续执行其中一个程序。

- 配置高级 ASA 子接口选项。高级设置的默认值适用于大多数网络。只有在需要解决网络问题时，再进行编辑。
- 如果您保存了子接口，并且不想继续使用高级子接口选项，请继续启用子接口。

配置高级 ASA 子接口选项

高级接口选项的默认设置适用于大多数网络。只有在需要解决网络问题时，再配置它们。

以下步骤程序假定已定义接口。另外，您还可以在初始编辑或创建接口时编辑这些设置。

此程序及其中的所有步骤都是可选的。

步骤 1 在**创建子接口 (Creating Subinterface)** 对话框中，点击**高级 (Advanced)** 选项卡。

步骤 2 配置以下高级设置：

- **HA 监控 (HA Monitoring)**：启用后，可在当 HA 对决定是否在高可用性配置中故障转移到对等设备时考虑接口的运行状况。如果不配置高可用性，可忽略此选项。如果不配置接口的名称，也可以忽略此选项。

- **仅管理 (Management Only)**：启用后，可进行数据接口管理。

  仅管理接口不允许直通流量，所以将数据接口设置为**仅管理 (Management Only)** 接口的价值微乎其微。不能更改管理/诊断接口的此项设置，它们始终为仅管理。

- **MTU**：默认 MTU 为 1500 字节。您可以指定 64 - 9198 之间的值。如果通常在网络中使用巨帧，请设置一个较大的值。

- **DAD 尝试 (DAD Attempts)**：接口执行重复地址检测 (DAD) 的频率，介于 0 - 600 之间。默认值为 1。在无状态自动配置过程中，DAD 会验证新单播 IPv6 地址的唯一性，再将地址分配给接口。如果重复地址是接口的链路本地地址，则在接口上禁用 IPv6 数据包处理。如果重复地址是全局地址，则将不使用该地址。接口将使用邻居的询求消息来执行重复地址检测。将该值设置为 0 可禁用重复地址检测 (DAD) 流程。

- **MAC 地址 (MAC Address)**：采用 H.H.H 格式的介质访问控制，其中 H 是 16 位十六进制数字。例如，您可以将 MAC 地址 00-0C-F1-42-4C-DE 输入为 000C.F142.4CDE。MAC 地址不能设置组播位，即左起第二个十六进制数字不能是奇数。

- **备用 MAC 地址 (Standby MAC Address)**：用于高可用性。如果主用设备发生故障切换，备用设备变为主用设备，则新的主用设备开始使用主用 MAC 地址，以最大限度地减少网络中断，而原来的主用设备使用备用地址。

步骤 3 如果您保存了接口并且不想继续使用高级接口选项，请继续启用子接口。

步骤 4 点击**保存 (Save)**。

启用子接口

步骤 1 选择要启用的子接口。

步骤 2 移动与接口逻辑名称关联的窗口右上角的**状态 (State)** 滑块。

步骤 3 查看和部署所做的更改。

删除 ASA 子接口

使用以下程序从 ASA 中删除子接口。

步骤 1 在 CDO 导航窗格，点击**清单 (Inventory)**。

步骤 2 点击 **ASA** 选项卡。

步骤 3 选择您要修改的设备，然后在右侧的**管理 (Management)** 窗格中点击**接口 (Interfaces)**。

步骤 4 在**接口 (Interfaces)** 页面上，展开与要删除的子接口链接的物理接口，然后选择该特定子接口。

步骤 5 在右侧的**操作 (Actions)** 窗格中，点击**删除 (Remove)**。

步骤 6 确认要删除 EtherChannel 接口，然后点击**删除 (Delete)**。

步骤 7 预览和部署所有设备的配置更改所做的更改。

关于 ASA EtherChannel 接口

802.3ad EtherChannel 是逻辑接口（称为端口通道接口），该接口由一组单独的以太网链路（通道组）组成，以便可以提高单个网络的带宽。配置接口相关功能时，可以像使用物理接口一样来使用端口通道接口。

最多可以配置 48 个 Etherchannel，具体取决于型号支持的接口数量。

链路汇聚控制协议

链路汇聚控制协议 (LACP) 将在两个网络设备之间交换链路汇聚控制协议数据单元 (LACPDU)，进而汇聚接口。

LACP 将协调自动添加和删除指向 EtherChannel 的链接，而无需用户干预。LACP 还会处理配置错误，并检查成员接口的两端是否连接到正确的通道组。如果接口发生故障且未检查连接和配置，“开启”模式将不能使用通道组中的备用接口。

有关 ASA EtherChannel 接口的详细信息，请参阅《ASDM 手册 1：思科 ASA 系列常规操作 ASDM 配置指南 X, Y》的 **EtherChannel 和冗余接口**一章。

配置 ASA EtherChannel

使用此程序将新的 EtherChannel 接口添加到 ASA。

开始之前

要在 ASA 接口上配置 EtherChannel，必须满足以下前提条件：

- 通道组中的所有接口都必须具有相同的介质类型和容量，并且必须设置为相同的速度和双工模式。介质类型可以是 RJ-45 或 SFP；可以混合使用不同类型（铜缆和光纤）的 SFP。不能通过在较大容量的接口上将速度设置为较低来混合接口容量（例如 1GB 和 10GB 接口），但 Cisco Secure Firewall 3100 除外，它支持不同的接口容量，只要速度设置为检测 SFP；在此情况下会使用较低的常见速度。
- 如果已为物理接口配置了名称，则不能将该物理接口添加到通道组。您必须先删除该名称。
- 不能添加另一个 EtherChannel 接口组的接口部分、交换机端口接口和具有子接口的接口。

步骤 1 在 CDO 导航窗格，点击**清单 (Inventory)**。

步骤 2 点击 **ASA** 选项卡。

步骤 3 选择您要修改的设备，然后在右侧的**管理 (Management)** 窗格中点击**接口 (Interfaces)**。

步骤 4 选择  > **EtherChannel 接口 (EtherChannel Interface)**。

步骤 5 在**逻辑名称 (Logical Name)** 字段中，提供 EtherChannel 接口的名称。

步骤 6 在**冗余 ID (Redundant ID)** 字段中，请输入一个介于 1 和 8 之间的整数。

步骤 7 点击**链路汇聚控制协议 (Link Aggregation Control Protocol)** 的下拉按钮，然后选择以下两个选项之一：

- **Active (活动)** - 发送和接收 LACP 更新。主用 EtherChannel 可以与主用或备用 EtherChannel 建立连接。除非您需要最大限度地减少 LACP 流量，否则应使用主用模式。
- **开 (On)** - EtherChannel 始终开启，并且不使用 LACP。**开启**的 EtherChannel 只能与另一个**开启**的 EtherChannel 建立连接。

步骤 8 搜索并选择要作为成员包含在 EtherChannel 中的接口。您**必须**包含至少一个接口。

警告 如果将 EtherChannel 接口添加为成员，并且该接口已配置了 IP 地址，则 CDO 会删除该成员的 IP 地址。

步骤 9 选择 **IPv4**、**IPv6** 或**高级 (Advanced)** 选项卡以配置子接口的 IP 地址。

- 如果要为 ASA EtherChannel 接口分配 IPv4 地址，请为 ASA 物理接口配置 IPv4 地址。
- 如果要为 ASA EtherChannel 接口分配 IPv6 地址，请为 ASA 物理接口配置 IPv6 地址。
- 配置高级 ASA 物理接口选项。高级设置的默认值适用于大多数网络。只有在需要解决网络问题时，再进行编辑。

步骤 10 移动窗口右上角的**状态 (State)** 滑块以启用 EtherChannel 接口。

步骤 11 点击**保存 (Save)**。

步骤 12 预览和部署所有设备的配置更改所做的更改。

编辑 ASA EtherChannel

使用此程序可编辑 ASA 上的现有 EtherChannel。

步骤 1 在 CDO 导航窗格，点击**清单 (Inventory)**。

步骤 2 点击 **ASA** 选项卡。

步骤 3 选择您要修改的设备，然后在右侧的**管理 (Management)** 窗格中点击**接口 (Interfaces)**。

步骤 4 在**接口 (Interfaces)** 页面上，选择要编辑的 EtherChannel 接口。

步骤 5 在位于右侧的**操作 (Actions)** 窗格中，点击**编辑 (Edit)**。

步骤 6 修改所需的值，然后点击**保存 (Save)**。

步骤 7 预览和部署所有设备的配置更改所做的更改。

移除 ASA EtherChannel 接口

使用以下程序从 ASA 中删除 EtherChannel 接口。

步骤 1 在 CDO 导航窗格，点击**清单 (Inventory)**。

步骤 2 点击 **ASA** 选项卡。

步骤 3 选择您要修改的设备，然后在右侧的**管理 (Management)** 窗格中点击**接口 (Interfaces)**。

步骤 4 在**接口 (Interfaces)** 页面上，选择要删除的 EtherChannel 接口。

步骤 5 在右侧的**操作 (Actions)** 窗格中，点击**删除 (Remove)**。

步骤 6 确认要删除 EtherChannel 接口，然后点击**删除 (Delete)**。

步骤 7 预览和部署所有设备的配置更改所做的更改。

ASA 系统设置策略

ASA 系统设置策略简介

使用系统设置策略来管理ASA设备的操作和功能。此策略包括基本配置，例如域名服务、启用安全复制服务器、消息日志记录以及允许 VPN 流量而不检查 ACL。通过设置策略，您可以确保正确配置设备以维护安全的网络环境。

在配置ASA设备时，请务必注意，您可以选择使用共享系统设置策略管理多个设备的设置，也可以单独编辑任何单个设备的设置。

共享系统设置策略

共享系统设置策略适用于网络中的多个ASA设备。通过它可以同时配置多个受管设备，从而在部署中提供一致性并精简管理工作。对共享策略的参数所做的任何更改都会影响使用该策略的其他 ASA 设备。

选择**策略 (Policies)** > **ASA 系统设置 (ASA System Settings)**。请参阅创建 ASA 共享系统设置策略，第 14 页。

您还可以修改特定于单个 ASA 设备的设备特定系统设置，以覆盖共享系统设置策略值。选择**清单 (Inventory)** > **ASA 设备 (ASA device)** > **管理 (Management)** > **设置 (Settings)**。请参阅配置或修改设备特定系统设置，第 21 页。

创建 ASA 共享系统设置策略

使用此部分为 ASA 设备创建新的共享系统设置策略。

步骤 1 选择**策略 (Policies)** > **ASA 系统设置 (ASA System Settings)**。

步骤 2 请点击  。

步骤 3 在**名称 (Name)** 字段中，输入策略的名称并点击**保存 (Save)**。

步骤 4 在编辑 ASA 共享系统设置页面中，配置所需的参数：

- 配置基本 DNS 设置，第 15 页

- 配置 HTTP 设置， 第 16 页
- 使用 NTP 服务器设置日期和时间， 第 16 页
- 配置 SSH 访问， 第 17 页
- 配置系统日志记录， 第 18 页
- 启用 Sysopt 设置， 第 20 页

注释

- 相应参数上的橙色点 ( ) 会突出显示未保存的更改。
- 被拒绝的符号 ( ) 突出显示了使用设备中现有本地值的参数。

配置基本 DNS 设置

需要配置 DNS 服务器，以便 ASA 能够将主机名解析为 IP 地址。还必须配置 DNS 服务器，以在访问规则中使用完全限定域名 (FQDN) 网络对象。

步骤 1 在编辑 ASA 系统设置页面中，点击左侧窗格中的 **DNS**。

步骤 2 取消选中**保留现有值 (Retain existing values)** 复选框以配置共享 ASA 系统设置策略的值。

重要事项 如果选中了**保留现有值 (Retain existing values)** 复选框，则无法配置值，因为字段已隐藏。对于此设置，CDO 会使用 ASA 设备的现有本地值，而不是从共享策略继承。

步骤 3 在 **DNS** 部分中，点击 以配置服务器。

- **IP 版本 (IP Version)**：选择要使用的 IP 地址版本。
- **IP 地址 (IP Address)**：指定 DNS 服务器的 IP 地址。
- **接口名称 (Interface Name)**：指定应启用 DNS 查找的接口。

注释 确保此处指定的接口名称在与此共享系统设置策略相关联的 ASA 设备上相同。

步骤 4 点击**保存 (Save)**。

步骤 5 在**域名 (Domain name)** 字段中，指定 ASA 的域名。

ASA 会将域名作为后缀追加到不受限定的名称。例如，如果您将域名设置为“example.com”并通过不受限定的名称“jupiter”来指定系统日志服务器，则 ASA 会将名称限定为“jupiter.example.com”。

步骤 6 在 **DNS 查找 (DNS Lookup)** 部分中，点击 并指定接口名称。

如果不在接口上启用 DNS 查找，则 ASA 将不会与该接口上的 DNS 服务器通信。确保在将用于访问 DNS 服务器的所有接口上启用 DNS 查找。

注释　　要删除配置的接口，您可以点击**操作 (Actions)** 下的删除图标。

步骤 7 点击**保存 (Save)**。

配置 HTTP 设置

要访问 ASA 接口以进行管理访问，您必须指定允许使用 HTTP 访问 ASA 的所有主机/网络的地址。如果您配置 HTTP 重定向以将 HTTP 连接自动重定向至 HTTPS，则必须启用允许 HTTP 的访问规则；否则，该接口无法侦听 HTTP 端口。

步骤 1 在编辑 ASA 系统设置页面中，点击左侧窗格中的 **HTTP**。

步骤 2 取消选中**保留现有值 (Retain existing values)** 复选框以配置共享 ASA 系统设置策略的值。

重要事项　　如果选中了**保留现有值 (Retain existing values)** 复选框，则无法配置值，因为字段已隐藏。对于此设置，CDO 会使用 ASA 设备的现有本地值，而不是从共享策略继承。

步骤 3 选中 **启用 HTTP 服务器** 复选框以启用 HTTP 服务器。

步骤 4 在**端口号 (Port Number)** 字段中，设置端口号。port 确定接口从其重定向 HTTP 连接的端口。

警告　　如果更改设备上的 HTTP 端口，则可能会导致其与 CDO 的连接出现一些问题。如果您计划更改与设备网络连接相关的任何设置，请务必记住这一点。

步骤 5 点击  添加 HTTP 信息。

- **接口 (Interface)**：确保此处指定的接口名称在与此共享系统设置策略相关联的 ASA 设备上相同。
- **IP 版本 (IP Version)**：选择要使用的 IP 地址版本。
- **IP 地址 (IP Address)**：指定可以使用 HTTP 访问 ASA 的所有主机/网络的地址。
- **网络掩码 (Netmask)**：指定网络子网掩码。

注释　　要删除主机，您可以点击**操作 (Actions)** 下的删除图标。

步骤 6 点击**保存 (Save)**。

使用 NTP 服务器设置日期和时间

NTP 用于实施分层服务器系统，可在网络系统中提供精确的同步时间。时间敏感性操作需要这种精确度，例如验证 CRL，其包括精确时间戳。可配置多个 NTP 服务器。ASA 选择层级最低的服务器，作为衡量数据可靠性的方式。

NTP 服务器生成的时间将覆盖手动设置的任何时间。

ASA 支持 NTPv4。

步骤 1 在编辑 ASA 系统设置页面中，点击左侧窗格中的 **NTP**。

步骤 2 取消选中**保留现有值 (Retain existing values)** 复选框以配置共享 ASA 系统设置策略的值。

重要事项 如果选中了**保留现有值 (Retain existing values)** 复选框，则无法配置值，因为字段已隐藏。对于此设置，CDO 会使用 ASA 设备的现有本地值，而不是从共享策略继承。

步骤 3 点击  以添加 NTP 服务器详细信息。

- **IP 版本 (IP Version)**：选择要使用的 IP 地址版本。
- **IP 地址 (IP Address)**：指定 NTP 服务器的 IP 地址。

  不能输入服务器的主机名；ASA 不支持 NTP 服务器的 DNS 查找。
- **密钥 ID (Key Id)**：输入一个介于 1 和 4294967295 之间的数字。

  该设置指定此身份验证密钥的密钥ID，可供您使用身份验证与NTP服务器进行通信。NTP服务器数据包必须也使用此密钥 ID。
- **接口名称 (Interface Name)**：指定接口名称。确保此处指定的接口名称在与此共享系统设置策略相关联的ASA设备上相同。

  NTP 使用一种算法确定最准确的服务器，然后与该服务器同步。如果多台服务器准确度相似，则使用首选服务器。但是，如果某台服务器的准确度明显高于首选服务器，则 ASA 将使用这台更准确的服务器。
- **首选 (Prefer)**：（可选）选中**首选 (Preferred)** 复选框，将该服务器设置为首选服务器。

注释 要删除 NTP 服务器，您可以点击**操作 (Actions)** 下的删除图标。

步骤 4 点击**保存 (Save)**。

配置 SSH 访问

您可以在 ASA 上启用安全复制 (SCP) 服务器。只有经允许使用 SSH 访问 ASA 的客户端才能建立安全复制连接。

步骤 1 在编辑 ASA 设置策略页面中，点击左侧窗格中的 **SSH**。

步骤 2 取消选中**保留现有值 (Retain existing values)** 复选框以配置共享 ASA 系统设置策略的值。

重要事项 如果选中了**保留现有值 (Retain existing values)** 复选框，则无法配置值，因为字段已隐藏。对于此设置，CDO 会使用 ASA 设备的现有本地值，而不是从共享策略继承。

步骤 3 启用**启用 Scopy SSH (Enable Scopy SSH)**（安全复制 SSH）。

步骤 4 在**超时时间 (Timeout in Minutes)** 字段中，将超时值设置为 1 到 60 分钟。默认值为 5 分钟。在大多数情况下，默认持续时间都太短，应增加为直到完成所有前期测试和故障排除所需的时间。

步骤 5 点击  并配置以下各项：

- **接口 (Interface)**：指定接口名称。确保此处指定的接口名称在与此共享系统设置策略相关联的 ASA 设备上相同。
- **IP 版本 (IP Version)**：选择要使用的 IP 地址版本。
- **IP 地址 (IP Address)**：指定可以使用 SSH 访问 ASA 的所有主机/网络的地址。
- **网络掩码 (Netmask)**：指定网络子网掩码。

注释　要删除 SSH 详细信息，您可以点击**操作 (Actions)** 下的删除图标。

步骤 6 点击**保存 (Save)**。

配置系统日志记录

系统日志记录是将来自设备的消息收集到运行系统日志后台守护程序的服务器的方法。将信息记录到中央系统日志服务器有助于汇聚日志和提醒。思科设备可以将其日志消息发送到 UNIX 样式的系统日志服务。系统日志服务接受消息并将其存储在文件中，或者根据简单配置文件打印消息。以这种形式记录日志可为日志提供受保护的长期存储。日志对常规故障排除及事件处理均有帮助。

安全级别

下表列出系统日志消息严重性级别。

表 *1:* 系统日志消息严重级别

级别号	安全等级	说明
0	应急	系统不可用
1	警报	需要立即采取措施。
2	严重	严重情况。
3	错误	错误情况。
4	警告	警告情况。
5	通知	正常但重大的情况。
6	信息性	消息仅供参考。
7	调试	消息仅供调试。 调试问题时，仅临时记录此级别的日志。此日志级别可能会生成太多消息，从而影响系统性能。

注释 ASA 不会生成严重性级别为零（紧急）的系统日志消息。

步骤 1 在编辑 ASA 系统设置页面中，点击左侧窗格中的**系统日志 (Syslog)**。

步骤 2 取消选中**保留现有值 (Retain existing values)** 复选框以配置共享 ASA 系统设置策略的值。

重要事项 如果选中了**保留现有值 (Retain existing values)** 复选框，则无法配置值，因为字段已隐藏。对于此设置，CDO 会使用 ASA 设备的现有本地值，而不是从共享策略继承。

步骤 3 进行以下配置：

- **日志记录已启用 (Logging Enabled)**：启用安全日志记录。
- **时间戳已启用 (Timestamp Enabled)**：启用后可在系统日志消息中包含日期和时间。
- **允许主机关闭 (Permit host down)**：（可选）禁用在 TCP 连接的系统日志服务器关闭时阻止新连接的功能。
- **缓冲区大小 (Buffer Size)**：指定内部日志缓冲区的大小。允许的范围为 4096 到 1048576 字节。
- **已缓冲的日志记录级别 (Buffered Logging Level)**：指定应将哪些系统日志记录消息发送到充当临时存储位置的内部日志缓冲区。
- **控制台日志记录级别 (Console Logging Level)**：指定应将哪些系统日志消息发送到控制台端口。
- **陷阱日志记录级别 (Trap Logging Level)**：指定应将哪些系统日志消息发送到系统日志服务器。

步骤 4 点击  以添加系统日志服务器详细信息。

- **接口名称 (Interface Name)**：指定系统日志服务器所在接口的名称。确保此处指定的接口名称在与此共享系统设置策略相关联的 ASA 设备上相同。
- **IP 版本 (IP Version)**：选择要使用的 IP 地址版本。
- **IP 地址 (IP Address)** - 指定系统日志服务器的 IP 地址。
- **协议 (Protocol)**：选择 ASA 应该用于将系统日志消息发送到系统日志服务器的协议（**TCP** 或 **UDP**）。
  - **端口 (Port)**：指定系统日志服务器为获取系统日志消息所侦听的端口。允许的 TCP 端口范围为 1 至 65535，UDP 端口范围为 1025 至 65535。
  - **思科 EMBLEM 格式的日志消息（仅限 UDP）(Log messages in Cisco EMBLEM format [UDP only])**：仅为带有 UDP 的系统日志服务器启用 EMBLEM 格式日志记录。
  - **使用 SSL 启用安全系统日志？(Enable secure syslog using SSL?)**：指定与远程日志记录主机的连接应仅对 TCP 使用 SSL/TLS。
- **引用身份 (Reference Identity)**：指定引用身份类型，以便根据先前配置的引用身份对象对证书进行 RFC 6125 引用身份检查。有关引用标识对象的详细信息，请参阅配置引用身份。

注释　　要删除系统日志服务器，您可以点击**操作 (Actions)** 下的删除图标。

步骤 5 点击**保存 (Save)**。

启用 Sysopt 设置

与传出接口绑定的加密映射 ACL 将允许或拒绝 IPSec 数据包通过 VPN 隧道。IPsec 对从 IPSec 隧道到达的数据包进行身份验证和解密，并使其按照与隧道关联的 ACL 接受评估。

ACL 定义要保护的 IP 流量。例如，您可以创建 ACL 以保护两个子网或两台主机之间的所有 IP 流量。

步骤 1 在编辑 ASA 系统设置页面中，点击左侧窗格中的 **Sysopt**。

步骤 2 取消选中**保留现有值 (Retain existing values)** 复选框以配置共享 ASA 系统设置策略的值。

重要事项　　如果选中了**保留现有值 (Retain existing values)** 复选框，则无法配置值，因为字段已隐藏。对于此设置，CDO 会使用 ASA 设备的现有本地值，而不是从共享策略继承。

步骤 3 启用**允许 VPN 流量绕行接口访问列表 (Allow VPN traffic to bypass interface access lists)** 会绕过 ACL 检查。

步骤 4 点击**保存 (Save)**。

从“共享系统设置”(Shared System Settings) 页面分配策略

在配置共享系统设置策略后，分配已载入的ASA设备并将设置部署到设备，以使更改生效。对策略所做的任何更改都会影响与该策略关联的设备。

您还可以从设备特定设置页面分配策略。

注释　　您只能将 ASA 设备关联到一个共享系统设置策略。

步骤 1 选择**策略 (Policies)** > **ASA 系统设置 (ASA System Settings)**。

步骤 2 选择共享策略，然后点击**编辑 (Edit)**。

步骤 3 点击策略名称旁边显示的过滤器以分配设备。

步骤 4 选择要与所选策略关联的 ASA 设备，然后点击**确定 (OK)**。

注释　　选中已与所选策略关联的设备的复选框。

如果您看到红色图标 ，则表示将共享系统设置策略应用于您的设备时发生错误。要解决问题，请点击**ASA 系统设置 (ASA System Settings)** 页面上的策略，然后在**检测到的错误 (Error Detected)** 窗格中点击**设备工作流程 (Device Workflows)** 以获取更多信息。

步骤 5 部署使用 CDO GUI 进行的配置更改所做的更改。

配置或修改设备特定系统设置

设备特定系统设置是 ASA 设备特定的现有值，可使用 CDO 进行修改。您可以使用所需参数的现有设备特定值来覆盖共享系统设置策略值。

本主题介绍如何配置已载入的 ASA 设备的系统设置。

步骤 1 在左侧窗格中，点击**清单 (Inventory)**。

步骤 2 点击 **ASA** 选项卡。

步骤 3 选择您想要的 ASA 设备，然后在右侧的**管理 (Management)** 窗格中点击**设置 (Settings)**。

您将看到所选 ASA 设备的设备特定系统设置。

注释 如果为所选设备分配了共享系统设置策略，**父策略**将提供打开该策略的链接。您还可以从设备特定的设置页面分配策略。选择要与所选策略关联的 ASA 设备，然后点击**确定 (OK)**

步骤 4 配置或修改所需的系统设置值，然后点击**保存 (Save)**。

注释 共享和设备特定系统设置的字段说明会保持不变。您可以点击下面的相应链接了解更多信息。

- 配置基本 DNS 设置， 第 15 页
- 配置 HTTP 设置， 第 16 页
- 使用 NTP 服务器设置日期和时间， 第 16 页
- 配置 SSH 访问， 第 17 页
- 配置系统日志记录， 第 18 页
- 启用 Sysopt 设置， 第 20 页

您可以点击**返回清单 (Return to Inventory)** 以导航至清单页面。

步骤 5 完成更改后点击**保存 (Save)**。

注释 相应参数上的橙色点 () 会突出显示未保存的更改。

从设备特定设置页面分配策略

您还可以从已载入的 ASA 设备的设备特定设置页面分配策略。

步骤 1 在左侧窗格中，点击**清单 (Inventory)**。

步骤 2 点击 **ASA** 选项卡。

步骤 3 选择您想要的 ASA 设备，然后在右侧的**管理 (Management)** 窗格中点击**设置 (Settings)**。

您将看到所选 ASA 设备的设备特定设置。

注释 如果为所选设备分配了共享系统设置策略，**父策略**将提供打开该策略的链接。选择要与所选策略关联的 ASA 设备，然后点击**确定 (OK)**

步骤 4 点击**父策略 (Parent Policy)** 按钮以分配共享系统设置策略。

步骤 5 选择策略，然后点击**应用 (Apply)**。

步骤 6 部署使用 CDO GUI 进行的配置更改所做的更改。

将 ASA 设备自动分配到共享系统设置策略

在载入新的 ASA 设备或检查更改或处理现有设备的带外更改时，CDO 会验证是否：

- 设备特定设置与预先存在的共享系统设置策略相匹配。如果匹配，设备将被分配到共享系统设置策略。
- 已载入设备的设备特定本地设置彼此匹配。如果是这样，则会自动创建一个新的共享系统设置策略，并将具有相同本地设置的设备分配给该共享策略。

注释 无论它是由用户还是系统创建的，您都可以重命名共享设置策略。

过滤 ASA 共享系统设置策略

如果您在ASA系统设置页面上搜索特定的共享系统设置策略，则可以使用基于问题和使用情况的过滤器来缩小搜索范围并更轻松地查找所需内容。

选择**策略 (Policies)**> **ASA 系统设置 (ASA System Settings)** > 。

- 问题：
  - **检测到的问题 (Issue Detected)**：仅显示在向其应用设备时存在问题的策略。
  - **无问题 (No issue)**：仅显示已成功应用于设备的策略。
- 用法：
  - **使用中 (In Use)**：显示已分配给设备的策略。
  - **未使用 (Unused)**：显示尚未分配给任何设备的策略。

将设备从共享系统设置策略取消关联

如果共享系统设置策略中不再需要ASA设备，则可以轻松地将其取消关联。在以下情况下，设备将从策略中分离：

- 对特定于设备的设置进行了更改，其中共享策略上的相应设置未配置为保留设备中的现有值。
- 设备从共享系统设置策略中手动分离。
- 共享系统设置策略已从 CDO 中删除。但是，这样不会删除设备。请参阅 删除共享设置策略，第 23 页。

步骤 1 选择**策略 (Policies)** > **ASA 系统设置 (ASA System Settings)**。

步骤 2 选择共享策略，然后点击**编辑 (Edit)**。

步骤 3 点击策略名称旁边显示的过滤器以分离设备。

步骤 4 取消选中要从所选共享系统设置策略中分离的设备，然后点击**确定 (OK)**。

注释 更改会自动保存，无需任何手动部署。

删除共享设置策略

如果要删除某些共享设置策略，您可以选择其中一个或多个策略并将其删除。但务必注意，只有在尚未将其应用或提交到任何设备的情况下，才能将其删除。

开始之前

确保设备已与要删除的共享设置策略取消关联。有关详细信息，请参阅将设备从共享系统设置策略取消关联。

步骤 1 选择**策略 (Policies)** > **ASA 系统设置 (ASA System Settings)**。

步骤 2 选择共享策略，然后点击**删除 (Delete)**。

步骤 3 点击**确定 (OK)** 以确认操作。

注释 如果从 CDO 中删除 ASA，则设备特定的设置和配置也将被删除，并且设备引用将从共享设置策略中删除。

ASA 路由

路由协议使用指标来评估传播数据包的最佳路径。指标是一种测量标准，例如供路由算法用于确定目标的最佳路径的路径带宽。为帮助执行确定路径的过程，路由算法会初始化和维护其中包含路由信息的路由表。路由信息根据所使用的路由算法而异。

路由算法使用各种信息来填充路由表。目标或下一跳关联告知路由器，可以通过将数据包发送到特定路由器（表示通往最终目标的下一跳）来以最优路径到达特定目标。当路由器收到传入数据包时，会检查目标地址并尝试将此地址与下一跳关联。

路由表还包含其他信息，例如有关路径可取性的数据。路由器通过比较指标来确定最佳路由，而这些指标根据所使用的路由算法的设计而异。

路由器互相进行通信，并通过传输各种消息来维护其路由表。路由更新消息是通常由路由表的全部或部分内容组成的消息。通过分析来自所有其他路由器的路由更新，路由器可以构建详细的网络拓扑图。链路状态通告（路由器之间发送的另一种消息）用于告知其他路由器发送方链路的状态。链路信息可用于构建完整网络拓扑图，以使路由器能够确定通向网络目标的最佳路径。

关于 ASA 静态路由

要将流量路由到非连接的主机或网络，必须使用静态路由或动态路由定义到主机或网络的路由。通常，您必须配置至少一个静态路由：所有流量的默认路由（不是通过其他方式路由到默认网络网关），通常是指下一跳路由器。

有关 ASA 如何路由的概念和 CLI 命令的一般信息，请参阅以下文档：

- ASDM 手册 1：《思科 ASA 系列通用操作 ASDM 配置指南 X,Y 版》的静态和默认路由一章。
- CLI 手册 1：《思科 ASA 系列通用操作 CLI 配置指南 X,Y 版》的静态和默认路由一章。

默认路由

最简单的方法是配置一个默认静态路由，将所有流量都发送到上游路由器，从而依靠该路由器来为您路由流量。默认路由对网关IP地址进行标识，ASA将所有不具有已获悉或静态路由的数据包发送到该网关地址。默认静态路由是以 0.0.0.0/0 (IPv4) 或 ::/0 (IPv6) 作为目标 IP 地址的静态路由。

应始终定义一个默认路由。

Static Route

在以下情况下，您可能希望使用静态路由：

- 您的网络使用不受支持的路由器发现协议。
- 网络规模较小，并且可以轻松管理静态路由。
- 不希望流量或 CPU 开销与路由协议相关联。

- 在某些情况下，仅使用默认路由并不足够。默认网关可能无法到达目标网络，因此还必须配置更具体的静态路由。例如，如果默认网关在外部，则默认路由无法将直接流量定向到未直接与 ASA 连接的任何内部网络。
- 您使用的是不支持动态路由协议的功能。

静态路由跟踪

使用静态路由的一个问题是，缺乏用于确定路由处于开启还是关闭状态的内在机制。即使下一跳网关变得不可用，这些路由依然保留在路由表中。只有当ASA上的关联接口发生故障时，才会从路由表中删除静态路由。

静态路由跟踪功能提供在主路由发生故障的情况下跟踪静态路由的可用性和安装备用路由的方法。例如，您可以定义一条到 ISP 网关的默认路由和一条到辅助 ISP的备用默认路由，以防主 ISP 不可用。

ASA 通过将静态路由与 ASA 使用 ICMP 回应请求监控的目标网络上的监控目标主机相关联来实施静态路由跟踪。如果在指定时间内没有收到回应回复，则主机将被视为关闭，并且会从路由表中删除关联路由。使用具有较高指标的未跟踪备用路由替代已删除的路由。

选择监控目标时，您需要确保它能够响应 ICMP 回应请求。该目标可以是您选择的任何网络对象，但是应考虑使用以下对象：

- ISP 网关（用于支持双 ISP）地址。
- 下一跳网关地址（如果您关注网关的可用性）。
- 目标网络上的服务器，例如 ASA 需要与之进行通信的系统日志服务器。
- 目标网络上的持久网络对象。

配置 ASA 静态路由

静态路由用于定义为特定目标网络发送流量的位置。

本节介绍将静态路由添加到 ASA 设备的步骤。

步骤 1 在左侧窗格中，点击**清单 (Inventory)**。

步骤 2 点击 **ASA** 选项卡。

步骤 3 选择要配置静态路由的设备。

步骤 4 在左侧的**管理 (Management)** 窗格中，点击**路由 (Routing)**。

步骤 5 点击  以添加静态路由。

步骤 6 您可以输入路由的**说明**。

步骤 7 选择路由是用于 **IPv4** 还是 **IPv6** 地址。

步骤 8 配置路由属性：

- **接口 (Interface)**：选择要通过其发送流量的接口。通过此接口需能够访问网关地址。

您可以使用 **Null0** 路由转发不必要或不需要的流量，从而丢弃该流量。静态 Null0 路由具有良好的性能配置文件。您还可以使用静态 null0 路由防止产生路由环路。

ASA CLI 接受 Null0 或 null0 字符串。

- **网关 IP (Gateway IP)**：（不适用于 **Null0** 路由）选择标识网关 IP 地址的主机网络对象至目标网络。流量将发送至此地址。
- **度量 (Metric)**：路由的管理距离，该值介于 1 和 254 之间。静态路由的默认值为 1。如果接口和网关之间还有其他路由器，请输入跳数作为管理距离。

  管理距离是用于比较路由的参数。数字越小，为该路由指定的优先级越高。连接的路由（直连到设备接口的网络）始终优先于静态路由。
- **目标 IP (Destination IP)**：选择标识目标网络的网络对象，该目标网络包含在此路由中使用网关的主机。
- **目标掩码 (Destination Mask)**（仅适用于 IPv4 寻址）：输入目的 IP 的子网掩码。
- **跟踪 (Tracking)**（仅适用于 IPv4 寻址）：输入路由跟踪进程的唯一标识符。

步骤 9 点击**保存 (Save)**。

步骤 10 部署使用 CDO GUI 进行的配置更改您所做的更改，或等待并一次部署多个更改。

编辑 ASA 静态路由

您可以编辑与 ASA 设备关联的静态路由参数。

注释 但是，在修改静态路由时不能选择其他 IP 版本。或者，您可以根据自己的要求创建新的静态路由。

步骤 1 选择要编辑静态路由的 ASA 设备。

步骤 2 在左侧的**管理 (Management)** 窗格中，点击**路由 (Routing)**。

步骤 3 在路由列表页面中，选择要修改的路由，然后在右侧的**操作 (Actions)** 窗格中，点击**编辑 (Edit)**。

步骤 4 修改所需的值，然后点击**保存 (Save)**。有关路由参数的信息，请参阅配置 ASA 静态路由，第 25 页。

步骤 5 部署使用 CDO GUI 进行的配置更改您所做的更改，或等待并一次部署多个更改。

删除静态路由

开始之前

删除静态路由可能会影响与设备的本地 SDC 或 CDO 的连接。确保为任何连接丢失制定了适当的灾难恢复程序。

步骤 1 选择要删除的 ASA 设备。

步骤 2 在左侧的**管理 (Management)** 窗格中，点击**路由 (Routing)**。

步骤 3 在路由列表页面中，选择要修改的路由，然后在右侧的**操作 (Actions)** 窗格中，点击**删除 (Delete)**。

步骤 4 点击“确定”(OK) 确认更改。

步骤 5 部署使用 CDO GUI 进行的配置更改您所做的更改，或等待并一次部署多个更改。

安全策略管理

安全策略检查网络流量，最终目标是允许流量到达其预定目的地，或者在识别出安全威胁时丢弃该流量。您可以使用 CDO 在许多不同类型的设备上配置安全策略。

- ASA 策略（扩展访问列表），第 37 页
- 网络地址转换，第 44 页

管理传统 ASA 访问策略

本部分提供有关传统网络策略页面的信息，该页面显示 Cisco Defense Orchestrator (CDO) 管理的所有设备正在使用的所有网络策略的列表。导航策略 ASA 策略以到达网络策略页面。 >

网络策略是网络规则的集合。每个网络规则根据源和目标 IP 地址、IP 协议、端口号、EtherType 等特征允许或阻止网络流量到达网络目标。

当 CDO 创建网络策略时，它会将其与 ASA 接口关联，并在策略中创建一个默认规则。与接口关联的网络策略是 ASA 所称的“访问组”。策略名称相当于 ASA 中的访问控制列表 (ACL) 名称。CDO 创建的默认规则以及您添加到此网络策略的后续规则在 ASA 中称为访问控制条目 (ACE)。访问控制条目 (ACE)，第 37 页

相关信息：

- 在传统视图中创建 ASA 网络策略
- 编辑 ASA 网络策略
- 复制 ASA 网络策略
- 比较 ASA 网络策略
- 删除 ASA 网络策略
- 搜索和过滤 ASA 网络策略和规则
- 共享 ASA 网络策略
- 访问控制条目 (ACE)

在传统视图中创建 ASA 网络策略

使用此程序创建 ASA 网络策略：

步骤 1 选择策略 ASA 策略。 >

步骤 2 点击**创建策略**。

步骤 3 点击设备过滤器以搜索您将在其上保存策略的设备。

步骤 4 输入策略的名称。请注意，一台设备上不能有两个具有相同名称的网络策略。

步骤 5 选择要应用此策略的接口。

步骤 6 指定策略是用于出站流量还是入站流量。请注意，同一设备上的同一接口不能有两个策略。

步骤 7 点击**保存 (Save)**。CDO 为该策略创建网络策略和单个“permit IP any any”规则。

步骤 8 根据需要编辑策略。编辑 ASA 网络策略, on page 28

步骤 9 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

编辑 ASA 网络策略

Defense Orchestrator 允许您从“策略详细信息”页面编辑网络策略和策略规则。您可以通过以下方式编辑 ASA 策略：

- 重命名策略
- 将规则添加到策略
- 在策略中移动规则
- 在策略之间移动规则
- 在策略中停用规则
- 记录规则活动
- 定义策略的时间范围

重命名策略

步骤 1 选择策略 ASA 策略。 >

步骤 2 选择要重命名的网络策略。

步骤 3 点击详细信息窗格中的重命名图标 。

步骤 4 编辑策略名称，然后点击蓝色复选框以保存更改。

将规则添加到策略

步骤 1 选择策略 > ASA 策略。

步骤 2 选择要编辑的网络策略。

步骤 3 点击**编辑策略 (Edit Policy)**。

步骤 4 在详细信息窗格中，点击编辑工具工具栏中的 ，将规则添加到网络策略。新规则将添加到策略中突出显示的规则上方。规则按规则列表中的位置确定优先级，从 1 到“最后”。

Note 默认情况下，为新规则分配“允许”操作。

步骤 5 点击**保存 (Save)**。Defense Orchestrator 可识别受更改影响的设备。

步骤 6 查看策略详细信息窗格中的设备字段。如果超过了最佳条目数，您将收到一条警告，例如“ACE count exceeded, 500 max entries, 1000 found”，具体取决于安装 ASA 的 ASA 硬件型号。

步骤 7 预览和部署所有设备的配置更改您现在所做的更改，或者等待并一次部署多个更改。

在策略中移动规则

步骤 1 选择策略 > ASA 策略。

步骤 2 选择网络策略。

步骤 3 在详细信息窗格中，点击编辑策略。

步骤 4 在规则表中选择一条规则，点击“编辑工具”栏中的“剪切”。

步骤 5 选择要在刚剪切的规则之前放置的规则。规则按规则列表中的位置确定优先级。数值越大，优先级越高。

步骤 6 点击粘贴。

步骤 7 点击**保存 (Save)**。Defense Orchestrator 可识别受更改影响的设备。

步骤 8 预览和部署所有设备的配置更改您现在所做的更改，或者等待并一次部署多个更改。

在策略之间移动规则

您可以复制一个策略中的规则并将其粘贴到另一个策略中。

步骤 1 选择策略 ASA 策略。 >

步骤 2 选择包含要复制的规则的网络策略。

步骤 3 在详细信息窗格中，点击编辑策略。

步骤 4 在规则表中选择一条规则，点击“编辑工具”栏中的复制。

步骤 5 选择策略 > ASA 策略。

步骤 6 选择要将规则复制到的网络策略。

步骤 7 在详细信息窗格中，点击编辑策略。

步骤 8 选择要放在刚刚复制的规则之后的规则。规则按规则列表中的位置确定优先级。数值越大，优先级越高。

步骤 9 点击粘贴。

步骤 10 点击**保存 (Save)**。Defense Orchestrator 可识别受更改影响的设备。

步骤 11 预览和部署所有设备的配置更改您现在所做的更改，或者等待并一次部署多个更改。

在策略中停用规则

默认情况下，规则处于活动状态。您可以停用策略中的单个规则。

步骤 1 选择策略 > ASA 策略。

步骤 2 选择包含要停用的规则的网络策略。

步骤 3 在详细信息窗格中，点击编辑策略。

步骤 4 选择要停用的规则。

步骤 5 关闭 Active 设置。

步骤 6 点击**保存 (Save)**。

步骤 7 点击**保存 (Save)**。Defense Orchestrator 可识别受更改影响的设备。

步骤 8 预览和部署所有设备的配置更改您现在所做的更改，或者等待并一次部署多个更改。

记录规则活动

默认情况下，不记录网络策略规则产生的活动。您可以为单个规则激活日志记录。

步骤 1 选择策略 ASA 策略。 >

步骤 2 选择包含要激活的规则的网络策略。

步骤 3 在详细信息窗格中，点击**编辑策略 (Edit Policy)**。

步骤 4 选择要记录活动的规则。

步骤 5 点击滑块以激活日志记录。

步骤 6 点击**编辑 (Edit)**。

步骤 7 选择从该规则收集活动的日志记录级别和频率。下表列出系统日志消息严重性级别。

严重性级别	说明
应急	系统不可用。
警报	需要立即采取措施。
严重	严重情况。

严重性级别	说明
错误	错误情况。
警告	警告情况。
通知	正常但重大的情况。
信息性	消息仅供参考。
调试	消息仅供调试。
Note	ASA 不会生成严重性级别为零（紧急）的系统日志消息。

步骤 8 您还可以更改日志记录间隔。日志记录间隔显示在该间隔内日志被命中的次数。日志记录间隔以秒为单位定义，范围为从 1 到 600。默认值为 300。此值也用作从用于收集丢弃统计信息的缓存中删除非活动的流的超时值。

步骤 9 点击**保存 (Save)**。Defense Orchestrator 可识别受更改影响的设备。

步骤 10 预览和部署所有设备的配置更改您现在所做的更改，或者等待并一次部署多个更改。

定义策略的时间范围

基于时间的ASA网络策略允许基于一天中的时间访问网络和资源。时间由时间范围对象定义。时间范围对象具有开始时间和结束时间，也可以定义为周期性事件。

如果已在 ASA 上定义时间范围对象，则可以将其与网络策略相关联。如果 ASA 上尚不存在时间范围对象，则必须使用 Defense Orchestrator 中的 CLI 工具创建它们，或直接在 ASA 上创建它们。

请按照以下程序为网络策略添加时间范围：

步骤 1 选择策略 ASA 策略。 >

步骤 2 选择要编辑的网络策略。

步骤 3 点击**编辑策略 (Edit Policy)**。

步骤 4 在网络策略框中，点击滑块以启用时间范围。

步骤 5 创建时间范围对象或从下拉列表中选择现有时间范围对象。

步骤 6 点击**保存 (Save)**。

步骤 7 返回到设备和服务页面，然后选择您刚刚对其进行策略编辑的设备。您应该会看到设备现在处于“未同步”(Not synced) 状态。

步骤 8 点击预览并部署...

步骤 9 在设备同步框中，查看将创建策略的命令和策略中的规则。

步骤 10 如果您对建议的更改感到满意，请点击将更改应用到设备。

步骤 11 预览和部署所有设备的配置更改您现在所做的更改，或者等待并一次部署多个更改。

复制 ASA 网络策略

使用此程序可将网络策略从一个 ASA 复制到另一个 ASA。

步骤 1 选择策略 ASA 策略。 >

步骤 2 搜索并过滤要复制的策略。

步骤 3 在要复制的网络策略所在的行中，点击复制图标。

步骤 4 将策略添加到设备：

- 对于分配给单个接口的网络策略：在将策略添加到设备对话框中，选择要将策略复制到的设备、接口和流量方向。如果要将全局访问策略复制到另一台设备
- 对于全局策略：在将策略添加到设备对话框中，选择要向其复制策略的设备，然后选中创建为全局策略。您会看到无法为策略选择接口或方向。全局策略始终分配给设备上的所有接口，并始终评估入站流量。

步骤 5 点击**保存 (Save)**。

步骤 6 立即 预览和部署所有设备的配置更改 您所做的更改，或等待并一次部署多个更改。

比较 ASA 网络策略

步骤 1 在导航窗格中，选择**策略 (Policies) > ASA 策略 (ASA Policies)**。

步骤 2 点击查看器右上角的**比较 (Compare)**。

步骤 3 最多选择两个要比较的策略。

步骤 4 点击查看器底部的**查看比较 (View Comparison)**。这将打开比较查看器。完成后，点击**完成 (Done)**，然后点击**完成比较 (Done Comparing)**。

删除 ASA 网络策略

步骤 1 在导航栏中，点击 **设备和服务**。

步骤 2 点击 **设备** 选项卡，找到您的设备。

步骤 3 点击 ASA 选项卡，搜索要从中删除策略的 ASA 并将其选中。

步骤 4 在管理窗格中，点击配置。

步骤 5 点击**编辑**。

步骤 6 在设备配置中，查找网络策略和规则。

网络策略在 ASA 配置文件中称为访问组，格式如下：

access-group < policy name > < direction of traffic > interface < interface name >

以下是访问组条目的示例：

```
access-group abc-75-1-out interface interface-1
```

网络规则在 ASA 配置文件中称为访问列表，格式如下：

```
access-list <policy name> extended permit ip any any
```

以下是访问列表条目的示例：

```
access-list abc-75-1-out extended permit ip any any
```

步骤 7 突出显示并删除包含网络策略的行和包含网络规则的行。

步骤 8 **保存**更改。

步骤 9 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

搜索和过滤 ASA 网络策略和规则

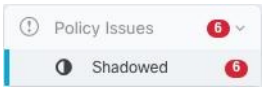
使用搜索栏在网络策略的名称和策略内的规则中搜索名称、关键字或短语。搜索不区分大小写。

过滤

使用过滤器边栏查找网络策略问题、共享策略以及特定设备上的策略。过滤不是相加的，每个过滤器设置相互独立。

政策问题

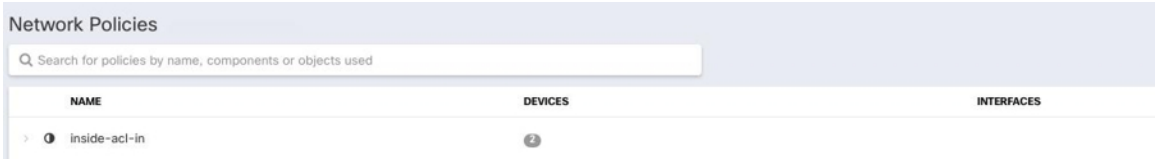
CDO 识别包含影子规则的网络策略。“策略问题”(Policy Issues) 过滤器中会指示包含影子规则的策略数量：



CDO 在网络策略页面上使用影子标记标记包含这些规则的影子规则和网络策略。◑点击已阴影 (Shadowed) 以查看包含阴影规则的所有策略。有关详细信息，请参阅影子规则。

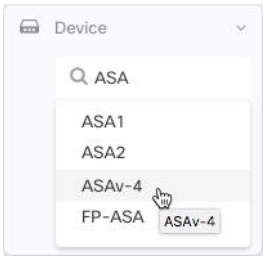
共享策略

共享策略是在多台设备上找到的策略。对共享策略所做的更改会影响找到该策略的所有设备。在下面的示例中，inside-acl-in 策略由两台设备共享。有关详细信息，请参阅共享 ASA 网络策略。



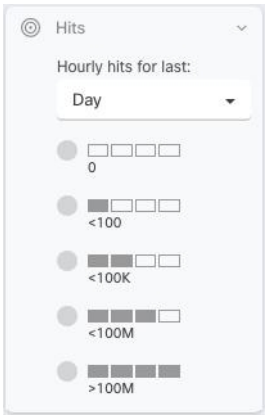
设备

通过展开设备过滤器，在搜索设备字段中输入名称或 IP 地址，然后选择在结果中找到的设备，按设备过滤网络策略列表。



点击数

使用此过滤器可查找在指定时间段内已触发多次的策略。



查找命中数为零的所有网络策略

如果您的网络策略没有任何命中，则可以对其进行编辑以使其更有效，也可以直接将其删除。

步骤 1 导航**策略 (Policies)** > **ASA 策略 (ASA Policies)**。

步骤 2 在过滤器窗格中，点击全部显示以清除任何现有过滤器。

步骤 3 展开 Hits 过滤器。

步骤 4 选择一个时间段

步骤 5 选择 0 个匹配项。

查找设备上命中数为零的所有网络策略

步骤 1 导航**策略 (Policies)** > **ASA 策略 (ASA Policies)**。

步骤 2 在过滤器窗格中，点击全部显示以清除任何现有过滤器。

步骤 3 展开设备过滤器，然后选择要过滤的设备。
步骤 4 展开 Hits 过滤器。
步骤 5 选择一个时间段
步骤 6 选择 0 个匹配项。

了解网络策略中的规则被命中的频率

步骤 1 导航**策略 (Policies)** > **ASA 策略 (ASA Policies)**。
步骤 2 在过滤器窗格中，点击全部显示以清除任何现有过滤器。
步骤 3 选择一台设备上使用的网络策略。
步骤 4 查看规则表的“命中”列，了解网络策略中每条规则的命中频率。
步骤 5 如果网络策略中的规则过多，无法一目了然地查看结果，请展开“命中”(Hits) 过滤器。
步骤 6 选择一个时间段
步骤 7 选择不同的命中过滤器，查看不同的规则所属的类别。

了解共享网络策略的命中频率

针对各个设备计算网络策略命中数。如果不指定过滤器中的设备，您将无法查看在两台或更多设备上共享的单个网络策略的命中率：

步骤 1 导航**策略** > **ASA 访问策略**。
步骤 2 在策略表上方，点击**清除**以清除任何现有过滤器
步骤 3 展开共享策略过滤器，然后点击**共享**。
步骤 4 选择共享网络策略。
步骤 5 在该策略的详细信息窗格中，记下使用该网络策略的设备，然后返回到网络策略表。
步骤 6 在搜索字段中输入共享策略名称。
步骤 7 展开设备过滤器，并按使用共享策略的设备之一进行过滤。
步骤 8 展开 Hits 过滤器
步骤 9 选择一个时间段
步骤 10 选择不同的命中过滤器以确定其所属的类别。

按命中率过滤网络策略

步骤 1 导航策略 ASA 访问策略。 >
步骤 2 在策略表上方，点击**清除 (Clear)** 以清除任何现有过滤器。

步骤 3 展开 Hits 过滤器。

步骤 4 选择时间段。

步骤 5 选择不同的命中率类别。CDO 显示以您指定的速率命中的策略。如果存在与命中率条件匹配的共享网络策略，则 CDO 会为使用该共享策略的每个设备显示一行。

共享 ASA 网络策略

Cisco Defense Orchestrator (CDO) 可查找多个 ASA 使用的相同网络策略，并在网络策略页面上进行标识。如果您有共享网络策略，则可以对其进行一次更改，并将更改分发到共享该策略的其他设备。这可以使各种设备的网络策略保持一致。

共享网络策略属性

网络策略表标识使用网络策略的设备数量。任何表明它被多个设备使用的网络策略都是共享策略。查找共享网络策略：

步骤 1 导航**策略 (Policies)** > **ASA 策略 (ASA Policies)**。

步骤 2 在过滤器窗格中，点击**全部显示 (Show All)** 以从页面中清除任何过去的过滤或搜索条件。

步骤 3 在过滤器栏中，展开共享策略并选择共享。

步骤 4 在搜索栏中输入关键字以进一步细化搜索。

步骤 5 从网络策略表中选择共享网络策略。

Note 过滤器和搜索条件不能组合使用，一次只能使用一个。例如，如果按“共享策略”进行过滤，则会看到所有共享策略。如果将设备名称添加到搜索中，无论策略是否共享，您都会看到该设备名称使用的所有网络策略。

编辑共享网络策略

步骤 1 查找要编辑的共享策略。共享 ASA 网络策略, on page 36

步骤 2 选择共享策略。CDO 标识 CDO 管理的哪些设备使用该网络策略。

步骤 3 在详细信息窗格中，点击**编辑策略 (Edit Policy)**。

步骤 4 编辑策略中的一个或多个规则。

步骤 5 点击**保存 (Save)**。

步骤 6 **确认**将受更改影响的设备。

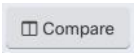
步骤 7 打开设备和服务页面，并注意设备不再同步。

步骤 8 点击**手动部署更改... (Deploy Changes Manually...)**，然后按照显示的说明使用您的更改更新 ASA 上保存的配置。

比较共享网络策略

比较共享网络策略的目的是找到略有差异的策略并重新调整它们。如果您有几个几乎相同的策略，则可能它们已经不同，它们实际上应该是相同的。重新调整网络策略后，CDO 会将这些策略识别为共享策略，当您更改策略时，您将能够使用该策略将更改分发到其他设备。

步骤 1 查找要比较的共享策略。共享 ASA 网络策略, on page 36

步骤 2 点击**比较 (Compare)** 

。

步骤 3 选择要比较的两个网络策略，然后点击查看比较。

步骤 4 记下差异，然后点击完成比较。

步骤 5 如果要更改其中一个策略以使其与另一个策略保持一致，请从网络策略表中选择该策略，然后点击详细信息窗格中的编辑策略进行编辑。

ASA 策略（扩展访问列表）

Cisco Defense Orchestrator (CDO) 为用户提供在所有设备上保持网络和应用安全策略一致的能力。借助此独特功能，可以轻松地同时跨多台设备更改策略。

访问控制条目 (ACE)

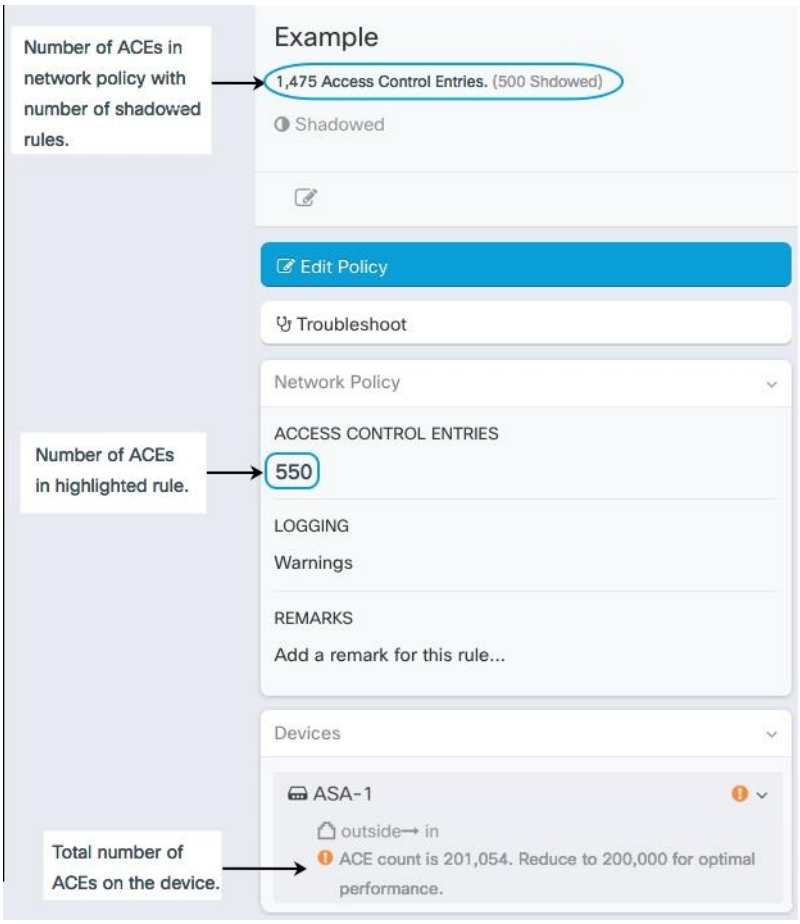
从您可以看到和看不到的方面考虑访问控制条目。

下面是您可以看到的内容。就 CDO 的用户界面而言，添加到网络策略的规则是 ASA 上的访问控制条目。该规则定义允许源地址和目的地址之间或一组地址和另一组地址之间的网络流量。

下面是您无法看到的内容。ASA 会扩展您创建的网络规则，以考虑网络规则隐含的每个可能的源 IP 地址和目标 IP 地址组合。例如，如果有一个规则，其中一个网络对象中的三个 IP 地址被拒绝访问另一个对象中的三个 IP 地址，则 ASA 会在内存中存储 9 个可能的访问控制条目。

ASA 可以处理的 ACE 数量没有硬编码限制，但当 ACE 数量过多时，ASA 性能会下降。请参阅表 4。有关特定 ASA 设备预期的最大 ACE 条目数，请参阅此自适应安全设备常见问题中的“思科 ASA 型号的最大访问控制条目数”。https://www.cisco.com/c/en/us/products/collateral/security/adaptive-security-appliance-asa-software/qa_c67-731962.html

CDO 维护从所有网络策略派生的 ACE 总数，并在 ACE 计数超过设备上预期的最大 ACE 限制时通知您。以下是 CDO 提供的信息：



减少设备上的 ACE 数量

以下是减少超过预期 ACE 最大数量的设备上的 ACE 数量的一些方法：

- 查找具有部分阴影和完全阴影规则的策略。影子规则，第 42 页如果合适，请删除这些规则。
- 过滤网络策略以查找设备上命中率为零的策略或查找命中率为零的规则。查找设备上命中数为零的所有网络策略，第 34 页了解网络策略中的规则被命中的频率，第 35 页删除命中数为零的策略或规则（如果合适）。
- 查找设备上超过预期访问控制条目数的所有网络策略，并查看这些策略。搜索和过滤ASA网络策略和规则，第 33 页考虑这些策略的源和目标寻址是否需要与您最初计划的一样广泛。

配置 ASA 全局访问策略

全局访问策略是应用于ASA上所有接口的网络策略。这些策略仅适用于入站网络流量。如果要将一组规则统一应用于所有 ASA 接口，请创建全局访问策略。

只能在 ASA 上配置一个全局访问策略。与任何其他策略一样，全局访问策略可以分配多个规则。

ASA 全局访问策略在特定接口的网络策略之后处理，在所有流量的隐式拒绝规则之前处理。以下是 ASA 上的规则处理顺序：

1. 接口访问规则。
2. 对于网桥组成员接口，网桥虚拟接口 (BVI) 访问规则。
3. 全局访问规则。
4. 隐式拒绝。

配置 ASA 全局访问策略的限制

CDO 允许您为 ASA 创建和编辑全局访问策略。但是，如果您的 ASA 在将其载入 CDO 时具有全局访问策略，则会受到以下限制：

- 您将能够编辑策略，但无法创建新策略，因为每台设备只允许一个全局访问策略。
- 如果 ASA 上的全局访问策略包含 CDO 不支持的规则，您将无法编辑该策略。
- 您只能使用 CLI 接口或通过编辑设备配置文件来删除策略。

创建全球访问策略

步骤 1 点击**策略 (Policies)** > **ASA 策略 (ASA Policies)**。

步骤 2 在过滤器面板中，过滤策略列表以查找要向其添加全局策略的设备。

步骤 3 在“网络策略”表的“接口”列中，确保没有标记为“全局”的策略。

步骤 4 点击**创建策略**。

步骤 5 点击设备按钮，然后选择要向其添加全局策略的 ASA。点击**选择**。

步骤 6 为策略指定名称，然后选中**创建为全局策略**。您会看到无法为策略选择接口或方向。全局策略始终分配给设备上的所有接口，并始终评估入站流量。

步骤 7 点击**保存 (Save)**。

步骤 8 使用 编辑 ASA 网络策略 将规则添加到新策略。

编辑全局访问策略

请牢记上述配置限制，使用“编辑 ASA 网络策略”(Edit an ASA Network Policy) 编辑全局访问策略。
编辑 ASA 网络策略, on page 28

Note 如果您发现由于 Edit Policy 按钮已停用而无法编辑全局策略，则可能是因为该策略是在 ASA 上创建的，并且包含具有 CDO 不支持的对象的规则。这些规则在全局访问策略表中不可见。在这种情况下，您需要使用 CDO 的 CLI 工具编辑配置文件，方法是使用 CDO 编辑 ASA 的配置文件，或直接在 ASA 上编辑全局策略。

将全局访问策略复制到另一台设备

使用 Copy an ASA Network Policy 将全局访问策略从一台设备复制到另一台设备，或将全局访问策略从一台设备复制到另一台设备上的单个接口。复制 ASA 网络策略, on page 32

删除全球访问策略

您无法使用 CDO 的用户界面删除全局访问策略。要删除全局访问策略，您需要使用 CDO 的 CLI 工具在命令行中删除全局访问策略，方法是使用 CDO 编辑 ASA 的配置文件，或直接在 ASA 上编辑全局策略。

命中率

CDO 使您能够在安全且可扩展的策略协调之上评估策略规则的结果，提供简单的可视化，以实现更准确的策略分析，并立即可操作地转向根本原因，所有这些都在云的单个窗格中。命中率功能使您能够：

- 消除过时和不匹配的策略规则，提高安全状态。
- 通过即时识别瓶颈以及确保实施正确有效的优先级来优化防火墙性能（例如，大多数触发的策略规则的优先级更高）。
- 在配置的数据保留期（1 年）内维护命中率信息的历史记录，即使在设备或策略规则重置时也是如此。
- 根据可操作的信息，加强对可疑的影子规则和未使用的规则的验证。消除对更新或删除的疑问。
- 在整个策略的上下文中可视化策略规则的使用情况，利用预定义的时间间隔（日、周、月、年）和实际命中的规模（零、> 100、> 100k 等）来评估对通过网络的数据包的影响。

查看 ASA 策略的命中率

步骤 1 从 CDO 菜单栏中选择策略 ASA 访问策略。 >

步骤 2 点击过滤器图标并将其固定为打开状态。

步骤 3 在命中 (Hits) 区域中，点击各种命中计数过滤器，以显示哪些策略的命中频率高于或低于其他策略。

导出网络策略规则

您可以将每个访问组或加密映射的内容导出到 .csv 文件。This.csv 显示每个访问控制列表 (ACL) 以及 CDO 具有的每个 ACL 的数据。

步骤 1 在导航窗格中，点击**策略 (Policies)** > **ASA 策略 (ASA Policies)**。

步骤 2 （可选）使用搜索和过滤 ASA 网络策略和规则过滤结果。

步骤 3 从结果中选择网络策略。

步骤 4 点击**导出到 CSV (Export to CSV)** 

。

步骤 5 CDO 会将您在屏幕上看到的规则导出至 .csv 文件。

将 ASA 策略更改应用于设备

当您在 Cisco Defense Orchestrator (CDO) 中修改安全策略时，更改会暂存到受影响的设备或服务。这会导致配置不同步。您可以通过在当前未同步的任何设备或服务上点击部署到设备...来查看并应用策略更改。

通过脚本部署到设备

完成 ASA 设备策略配置更改后，需要查看更改并将其应用于设备。

步骤 1 导航到设备选项卡，然后点击设备选项卡。

步骤 2 点击相应的设备类型选项卡，然后从表中选择修改的设备。配置状态应显示未同步，表示它具有尚未应用于设备的更改。

步骤 3 点击右侧栏中的同步，生成将应用于设备的命令，以使其与 CDO 配置处于同步状态。

步骤 4 出现提示时，点击下载命令 (Download Commands) 在本地下载命令的副本。这些命令将包含在文本文件中，可以在应用之前进行查看。如果需要，还将生成命令以恢复更改。

步骤 5 在 CDO 之外，使用标准协议登录设备，并应用下载的命令。

步骤 6 输入所有命令后，返回到 CDO 并再次在设备选项卡上选择修改的设备。

步骤 7 点击刷新以确认与 CDO 同步。

如果执行了部分命令或在带外执行了其他命令，则CDO通过打开一个显示差异的窗口来指示差异，并通过提供名为“检测到冲突”的更新状态来提醒用户。

ASA 策略中的安全组标记

如果您载入的 ASA 在其访问控制规则中使用安全组对象组（以下称为“SGT 组”）中的安全组标记，则思科 Defense Orchestrator 允许您编辑使用这些 SGT 组的规则并管理策略有这些规则。但是，您无法使用 CDO GUI 创建或编辑 SGT 组。要创建或编辑 SGT 组，您需要使用 ASA 的自适应安全设备管理器 (ASDM) 或 CDO 中提供的命令行接口。

在 CDO 的对象页面中，当阅读 SGT 组的详细信息时，您会看到这些对象被标识为系统提供的不可编辑的对象。

CDO 管理员可以对包含 SGT 组的 ACL 和 ASA 策略执行以下任务：

- CDO 管理员可以编辑 ACL 的所有方面，但源和目标安全组除外。
- 将包含 SGT 组的策略从一个 ASA 复制到另一个 ASA。

有关使用命令行接口配置思科 TrustSec 的详细说明，请参阅适用于您的 ASA 版本的《ASA CLI 手册 2：思科 ASA 系列防火墙 CLI 配置指南》的“ASA 和思科 TrustSec”一章。

影子规则

具有影子规则的网络策略是指策略中至少有一个规则永远不会触发，因为它前面的规则会阻止数据包被影子规则评估。

例如，请考虑“示例”网络策略中的这些网络对象和网络规则：

```
object network 02-50
range 10.10.10.2 10.10.10.50
object network 02-100
range 10.10.10.2 10.10.10.100
```

```
access-list example extended deny ip any4 object 02-50
access-list example extended permit ip host 10.10.10.35 object 02-50
access-list example extended permit ip any4 object 02-100
```

此规则不会评估任何流量，

```
access-list example extended permit ip host 10.10.10.35 object 02-50
```

因为之前的规则

```
access-list example extended deny ip any4 object 02-50
```

拒绝任何 ipv4 地址访问 10.10.10.2 - 10.10.10.50 范围内的任何地址。

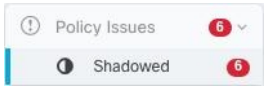
查找具有影子规则的网络策略

要查找包含影子规则的网络策略，请使用网络策略过滤器：

步骤 1 在导航窗格中，点击**策略 (Policies)** > **ASA 策略 (ASA Policies)**。

步骤 2 点击 ASA 访问策略表顶部的过滤器图标。

步骤 3 在“策略问题”(Policy Issues) 过滤器中，选中已阴影 (Shadowed) 以查看具有阴影规则的所有策略。



解决影子规则的问题

以下是 CDO 显示上述“示例”网络策略中所述规则的方式：

第 1 行的规则标有影子警告标志，因为它会影响策略中的另一条规则。⚠第 2 行的规则被标记为被策略中的另一条规则覆盖。◑第 2 行规则的操作显示为灰色，因为它完全被策略中的另一个规则所掩盖。CDO 能够告诉您策略中的哪条规则会影响第 2 行中的规则。

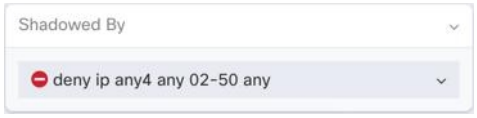
第3行的规则只能在某些时候触发。这是部分阴影规则。任何 IPv4 地址尝试到达 10.10.10.2-10.10.10.50 范围内的 IP 地址的网络流量都不会被评估，因为它已被第一条规则拒绝。但是，任何尝试访问 10.10.10.51-10.10.10.100 范围内的地址的 IPv4 地址都将通过最后一条规则进行评估，并被允许。

⚠

Caution CDO 不会将影子警告标志应用于部分影子规则。⚠

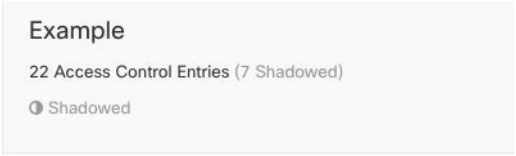
步骤 1 选择策略中的影子规则。在上面的示例中，这意味着点击第 2 行。

步骤 2 在规则详细信息窗格中，查找Shadowed By 区域。在本示例中，第 2 行中的规则的阴影部分区域显示它被第 1 行中的规则阴影：



步骤 3 查看 shadow 规则。是否太宽泛？查看 shadow ed 规则。您真的需要它吗？编辑 shadow 规则或删除 shadow ed 规则。

Note 通过删除影子规则，可以减少 ASA 上的访问控制条目 (ACE) 数量。这为创建其他 ACE 的规则释放了空间。CDO 计算从网络策略中的所有规则派生的 ACE 数量，并在网络策略详细信息窗格的顶部显示该总数。如果网络策略中的任何规则被映射，它也会列出该编号。



CDO还显示从网络策略中的单个规则派生的ACE数量，并在网络策略详细信息窗格中显示该信息。以下是该列表的示例：

步骤 4 通过查看网络策略详细信息窗格的设备区域，确定哪些设备使用该策略。

步骤 5 打开设备和服务页面，然后将更改部署回受策略更改影响的设备。

网络地址转换

IP 网络中的每台计算机和设备都分配了标识主机的唯一 IP 地址。因为缺乏公用 IPv4 地址，所以这些 IP 地址中的大多数都是专用地址，在专用公司网络以外的任何地方都不可路由。RFC 1918 定义可以在内部使用但不应通告的专用 IP 地址：

- 10.0.0.0 到 10.255.255.255
- 172.16.0.0 至 172.31.255.255
- 192.168.0.0 到 192.168.255.255

网络地址转换 (NAT) 的主要功能之一是使专用 IP 网络可以连接到互联网。NAT 用公用 IP 地址替换专用 IP 地址，将内部专用网络中的专用地址转换为可在公用互联网上使用的合法可路由地址。NAT 以此方式保存公用地址，因为它可配置为至少仅将整个网络的一个公用地址向外界通告。

NAT 的其他功能包括：

- 安全-隐藏内部 IP 地址可以阻止直接攻击。
- IP 路由解决方案-使用 NAT 时不会出现重叠 IP 地址。
- 灵活性-可以更改内部 IP 寻址方案，而不影响外部的可用公用地址；例如，对于可以访问互联网的服务器，可以维护供互联网使用的固定 IP 地址，但在内部，可以更改服务器地址。
- 在 IPv4 和 IPv6 之间转换（仅路由模式）- 如果想将 IPv6 网络连接到 IPv4 网络，可以利用 NAT 在两种类型的地址之间转换。

您可以使用 Cisco Defense Orchestrator 为许多不同的使用案例创建 NAT 规则。使用 NAT 规则向导或以下主题创建不同的 NAT 规则：

NAT 规则的处理顺序

网络对象 NAT 和两次 NAT 规则存储在划分为三部分的单个表中。首先应用第一部分规则，其次是第二部分，最后是第三部分，直到找到匹配项为止。例如，如果在第一部分找到匹配项，则不评估第二部分和第三部分。下表显示每个部分的规则顺序。

***Table 2: NAT* 规则表**

表部分	规则类型	部分中的规则顺序
第 1 部分	两次 NAT (ASA) 手动 NAT (FTD)	系统按照在配置中出现的顺序应用第一个匹配的规则。因为会应用第一个匹配规则，所以必须确保具体规则位于更加通用的规则前面，否则无法按预期应用特定规则。默认情况下，两次 NAT 规则会添加到第 1 部分。
第 2 部分	网络对象 NAT (ASA) 自动 NAT (FTD)	如果在第 1 部分未找到匹配项，则会按照以下顺序应用第 2 部分的规则： **1.** 静态规则。 **2.** 动态规则。 **在每个规则类型中，遵循以下排序准则：** **1.** 实际IP地址数量â€”从最小到最大。例如，带一个地址的对象将在带 10 个地址的对象之前进行评估。 **2.** 如果数量相同，则按从最低到最高的顺序使用 IP 地址编号。例如，10.1.1.0 在 11.1.1.0 之前进行评估。 **3.** 如果使用同一 IP 地址，则按字母数字顺序使用网络对象名称。例如，先评估对象“Arlington”，然后再评估对象“Detroit”。
第 3 部分	两次 NAT (ASA) 手动 NAT (FTD)	如果仍未找到匹配项，则按照在配置中出现的顺序，应用第三部分规则的第一个匹配项。此部分应当包含最通用的规则。还必须确保此部分的特定规则位于通用规则之前，否则会应用通用规则。

例如，对于第二部分规则，在网络对象中定义以下 IP 地址：

- 192.168.1.0/24（静态）
- 192.168.1.0/24（动态）

- 10.1.1.0/24（静态）
- 192.168.1.1/32（静态）
- 172.16.1.0/24（动态）（对象 Drtroit）
- 172.16.1.0/24（动态）（对象 Arlington）

结果排序可能是：

- 192.168.1.1/32（静态）
- 10.1.1.0/24（静态）
- 192.168.1.0/24（静态）
- 172.16.1.0/24（动态）（对象 Arlington）
- 172.16.1.0/24（动态）（对象 Drtroit）
- 192.168.1.0/24（动态）

网络地址转换向导

网络地址转换 (NAT) 向导可帮助您在设备上为以下类型的访问创建 NAT 规则：

- 为内部用户启用互联网访问。您可以使用此 NAT 规则允许内部网络上的用户访问互联网。
- 向互联网公开内部服务器。您可以使用此 NAT 规则允许网络外部的人员访问内部 Web 或邮件服务器。

“为内部用户启用互联网访问”的前提条件

在创建 NAT 规则之前，请收集以下信息：

- 最接近用户的接口；这通常称为“内部”接口。
- 离您的互联网连接最近的接口；这通常称为“外部”接口。
- 如果您只想允许特定用户访问互联网，则需要这些用户的子网地址。

“将内部服务器暴露给互联网”的必备条件

在创建 NAT 规则之前，请收集以下信息：

- 最接近用户的接口；这通常称为“内部”接口。
- 离您的互联网连接最近的接口；这通常称为“外部”接口。
- 要转换为面向互联网的 IP 地址的网络内服务器的 IP 地址。
- 您希望服务器使用的公共 IP 地址。

后续操作

请参阅使用 NAT 向导创建 NAT 规则, on page 47。

使用 NAT 向导创建 NAT 规则

Before you begin

有关使用 NAT 向导创建 NAT 规则所需的必备条件，请参阅网络地址转换向导, on page 46。

步骤 1 在 CDO 导航栏中，点击**清单 (Inventory)**。

步骤 2 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

步骤 3 点击设备类型选项卡。

步骤 4 使用过滤器和搜索字段查找要为其创建 NAT 规则的设备。

步骤 5 在详细信息面板的**管理 (Management)** 区域中，点击 **NAT** NAT。

步骤 6 点击 > NAT 向导。 

步骤 7 回答 NAT 向导问题并按照屏幕上的说明进行操作。

- NAT 向导创建规则。网络对象从下拉菜单中选择现有对象，或使用创建按钮创建新对象。 + Create...
- 在保存 NAT 规则之前，需要将所有 IP 地址定义为网络对象。

步骤 8 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

NAT 常见使用案例

两次 NAT 和手动 NAT

以下是使用“网络对象 NAT”（也称为“自动 NAT”）可以实现的一些常见任务：

- 启用内部网络上的服务器以使用公共 IP 地址访问互联网， 第 48 页
- 使内部网络上的用户能够使用外部接口的公共 IP 地址访问互联网， 第 49 页
- 使内部网络上的服务器在公共 IP 地址的特定端口上可用， 第 50 页
- 将专用 IP 地址范围转换为公用 IP 地址范围， 第 54 页

网络对象 NAT 和自动 NAT

以下是使用“两次 NAT”（也称为“手动 NAT”）可以实现的常见任务：

- 防止在遍历外部接口时转换某个范围的 IP 地址， 第 55 页

启用内部网络上的服务器以使用公共 IP 地址访问互联网

使用案例

当您的服务器具有需要从互联网访问的私有 IP 地址，并且您有足够的公共 IP 地址将一个公共 IP 地址转换为私有 IP 地址时，请使用此 NAT 策略。如果您的公共 IP 地址数量有限，请参阅使内部网络上的服务器在公共 IP 地址的特定端口上可用（该解决方案可能更合适）。

战略

您的服务器具有静态专用 IP 地址，网络外部的用户必须能够访问您的服务器。创建将静态私有 IP 地址转换为静态公共 IP 地址的网络对象 NAT 规则。之后，创建允许来自该公共 IP 地址的流量到达专用 IP 地址的访问策略。最后，将这些更改部署到您的设备。

Before you begin

在开始之前，请创建两个网络对象。将一个对象命名为 servername _inside，将另一个对象命名为 _outside。servername _inside 网络对象应包含服务器的专用 IP 地址。servername _outside 网络对象应包含服务器的公共 IP 地址。有关说明，请参阅创建网络对象。

步骤 1 在 CDO 导航栏中，点击**清单 (Inventory)**。

步骤 2 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

步骤 3 点击设备类型选项卡。

步骤 4 选择要为其创建 NAT 规则的设备。

步骤 5 点击右侧**管理 (Management)** 窗格中的 **NAT**。

步骤 6 点击 > 网络对象 NAT。 

步骤 7 在第 1 部分中，**键入**选择**静态 (Static)**。点击**继续 (Continue)**。

步骤 8 在部分 2 中，为源接口选择内部，为目标接口选择外部。点击**继续 (Continue)**。

步骤 9 在第 3 部分“数据包”中，执行以下操作：

a. 展开 Original Address 菜单，点击 Choose，然后选择 servername_inside 对象。

b. 展开 Translated Address 菜单，点击 Choose，然后选择 servername_outside 对象。

步骤 10 跳过第 4 节“高级”。

步骤 11 对于 FDM 管理的设备，在部分 5 (Name) 中，为 NAT 规则指定名称。

步骤 12 点击**保存 (Save)**。

步骤 13 对于ASA，部署网络策略规则，或者对于FDM管理设备，部署访问控制策略规则，以允许流量从*servername*_inside流向 *servername*_outside。

步骤 14 立即 预览和部署所有设备的配置更改 您所做的更改，或等待并一次部署多个更改。

ASA 的已保存配置文件中的条目

以下是由于此程序而创建并显示在 ASA 的已保存配置文件中的条目。

Note 这不适用于设备。FDM 管理

通过此程序创建的对象：

```
object network servername_outside
host 209.165.1.29
object network servername_inside
host 10.1.2.29
```

此程序创建的 *NAT* 规则：

```
object network servername_inside
 nat (inside,outside) static servername_outside
```

使内部网络上的用户能够使用外部接口的公共 IP 地址访问互联网

使用案例

通过共享外部接口的公共地址，允许专用网络中的用户和计算机连接到互联网。

战略

创建端口地址转换 (PAT) 规则，允许专用网络上的所有用户共享设备的外部接口公共 IP 地址。

将私有地址映射到公有地址和端口号后，设备会记录该映射。当收到发往该公共 IP 地址和端口的传入流量时，设备会将其发送回请求它的私有 IP 地址。

步骤 1 在 CDO 导航栏中，点击**清单 (Inventory)**。

步骤 2 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

步骤 3 点击设备类型选项卡。

步骤 4 选择要为其创建 NAT 规则的设备。

步骤 5 点击右侧**管理 (Management)** 窗格中的 **NAT**。

步骤 6 点击网络对象 NAT。 

步骤 7 在第 1 部分中，**键入**选择**动态 (Dynamic)**。点击**继续 (Continue)**。

步骤 8 在部分 2 中，为源接口选择 any，为目标接口选择 outside。点击**继续 (Continue)**。

步骤 9 在第 3 部分“数据包”中，执行以下操作：

a. 展开 Original Address 菜单，点击 Choose 并根据您的网络配置选择 any-ipv4 或 any-ipv6 对象。

b. 展开 Translated Address 菜单，然后从可用列表中选择 interface。接口指示使用外部接口的公共地址。

步骤 10 对于 FDM 托管设备，在第 5 部分**名称 (Name)**中，为 NAT 规则指定一个名称。

步骤 11 点击**保存 (Save)**。

步骤 12 立即 预览和部署所有设备的配置更改 您所做的更改，或等待并一次部署多个更改。

ASA 的已保存配置文件中的条目

以下是由于此程序而创建并显示在 ASA 的已保存配置文件中的条目。

Note 这不适用于设备。FDM 管理

通过此程序创建的对象：

```
object network any_network
subnet 0.0.0.0 0.0.0.0
```

此程序创建的 *NAT* 规则：

```
object network any_network
nat (any,outside) dynamic interface
```

使内部网络上的服务器在公共 IP 地址的特定端口上可用

使用案例

如果您只有一个或非常有限的公共 IP 地址，则可以创建一个网络对象 NAT 规则，将绑定到静态 IP 地址和端口的入站流量转换为内部地址。我们提供了适用于特定情况的程序，但您可以将其用作其他受支持应用的模型。

前提条件

在开始之前，请创建三个单独的网络对象，分别用于 FTP、HTTP 和 SMTP 服务器。出于以下程序的考虑，我们将这些对象称为 ftp-server-object、http-server-object 和 smtp-server-object。有关说明，请参阅创建网络对象。

到 FTP 服务器的 NAT 传入 FTP 流量

步骤 1 在 CDO 导航栏中，点击**清单 (Inventory)**。

步骤 2 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

步骤 3 点击设备类型选项卡。

步骤 4 选择要为其创建 NAT 规则的设备。

步骤 5 点击右侧**管理 (Management)** 窗格中的 **NAT**。

步骤 6 点击 > 网络对象 NAT。 

步骤 7 在第 1 部分中，**键入**选择**静态 (Static)**。点击**继续 (Continue)**。

步骤 8 在部分 2 中，为源接口选择内部，为目标接口选择外部。点击**继续 (Continue)**。

步骤 9 在第 3 部分“数据包”中，执行以下操作：

- 展开 Original Address 菜单，点击 **Choose**，然后选择 **ftp-server-object**。
- 展开 Translated Address 菜单，点击 **Choose**，然后选择 **Interface**。

- 选中使用端口转换 **(Use Port Translation)**。
- 选择 **tcp**、**ftp, ftp**。

步骤 10 跳过第 4 节“高级”。

步骤 11 对于 FDM 管理的设备，在部分 5 (Name) 中，为 NAT 规则指定名称。

步骤 12 点击保存 **(Save)**。新规则在 NAT 表的NAT 规则的处理顺序中创建。

步骤 13 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

ASA 的已保存配置文件中的条目

以下是由于此程序而创建并显示在 ASA 的已保存配置文件中的条目。

Note 这不适用于FDM 管理设备。

此程序创建的对象

```
object network ftp-object
host 10.1.2.27
```

此程序创建的 *NAT* 规则

```
object network ftp-object
nat (inside,outside) static interface service tcp ftp ftp
```

流向 HTTP 服务器的 NAT 传入 HTTP 流量

如果您只有一个或非常有限的公共 IP 地址，则可以创建一个网络对象 NAT 规则，将绑定到静态 IP 地址和端口的入站流量转换为内部地址。我们提供了适用于特定情况的程序，但您可以将其用作其他受支持应用的模型。

Before you begin

在开始之前，为 http 服务器创建网络对象。在本程序中，我们将调用对象 **http-object**。有关说明，请参阅创建网络对象。

步骤 1 在 CDO 导航栏中，点击清单 **(Inventory)**。

步骤 2 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

步骤 3 点击设备类型选项卡。

步骤 4 选择要为其创建 NAT 规则的设备。

步骤 5 点击右侧管理 **(Management)** 窗格中的 **NAT**。

步骤 6 点击 > 网络对象 NAT。 

步骤 7 在第 1 部分中，键入选择**静态 (Static)**。点击**继续 (Continue)**。

步骤 8 在部分 2 中，为源接口选择内部，为目标接口选择外部。点击**继续 (Continue)**。

步骤 9 在第 3 部分“数据包”中，执行以下操作：

- 展开 Original Address 菜单，点击 **Choose**，然后选择 **http** 对象。
- 展开 Translated Address 菜单，点击 **Choose**，然后选择 **Interface**。
- 选中**使用端口转换 (Use Port Translation)**。
- 选择 **tcp**、**http**、http。

步骤 10 跳过第 4 节“高级”。

步骤 11 对于 FDM 管理的设备，在部分 5 (Name) 中，为 NAT 规则指定名称。

步骤 12 点击**保存 (Save)**。新规则在 NAT 表的NAT 规则的处理顺序中创建。

步骤 13 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

ASA 的已保存配置文件中的条目

以下是由于此程序而创建并显示在 ASA 的已保存配置文件中的条目。

Note 这不适用于FDM 管理设备。

此程序创建的对象

```
object network http-object
host 10.1.2.28
```

此程序创建的 *NAT* 规则

```
object network http-object
nat (inside,outside) static interface service tcp www www
```

到 SMTP 服务器的 NAT 传入 SMTP 流量

如果您只有一个或非常有限的公共 IP 地址，则可以创建一个网络对象 NAT 规则，将绑定到静态 IP 地址和端口的入站流量转换为内部地址。我们提供了适用于特定情况的程序，但您可以将其用作其他受支持应用的模型。

Before you begin

在开始之前，为 SMTP 服务器创建网络对象。在本程序中，我们将调用对象 **smtp-object**。有关说明，请参阅创建网络对象。

步骤 1 在 CDO 导航栏中，点击**清单 (Inventory)**。

步骤 2 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

步骤 3 点击设备类型选项卡。

步骤 4 选择要为其创建 NAT 规则的设备。

步骤 5 点击右侧**管理 (Management)** 窗格中的 **NAT**。

步骤 6 点击 > 网络对象 NAT。 

步骤 7 在第 1 部分中，**键入选择静态 (Static)**。点击**继续 (Continue)**。

步骤 8 在部分 2 中，为源接口选择内部，为目标接口选择外部。点击**继续 (Continue)**。

步骤 9 在第 3 部分“数据包”中，执行以下操作：

- 展开 Original Address 菜单，点击 **Choose**，然后选择 smtp-server-object。
- 展开 Translated Address 菜单，点击 **Choose**，然后选择 **Interface**。
- 选中**使用端口转换 (Use Port Translation)**。
- 选择 **tcp**、**smtp**、**smtp**。

步骤 10 跳过第 4 节“高级”。

步骤 11 对于 FDM 管理的设备，在部分 5 (Name) 中，为 NAT 规则指定名称。

步骤 12 点击**保存 (Save)**。新规则在 NAT 表的NAT 规则的处理顺序中创建。

步骤 13 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

ASA 的已保存配置文件中的条目

以下是由于此程序而创建并显示在 ASA 的已保存配置文件中的条目。

Note 这不适用于FDM 管理设备。

此程序创建的对象

```
object network smtp-object
host 10.1.2.29
```

此程序创建的 *NAT* 规则

```
object network smtp-object
nat (inside,outside) static interface service tcp smtp smtp
```

将专用 IP 地址范围转换为公用 IP 地址范围

使用案例

如果您有一组特定设备类型或用户类型，需要将其 IP 地址转换为特定范围，以便接收设备（事务另一端的设备）允许流量传入。

将内部地址池转换为外部地址池

Before you begin

为要转换的私有 IP 地址池创建网络对象，并为要将这些私有 IP 地址转换为的公有地址池创建网络对象。

对于ASA，“原始地址”池（要转换的私有IP地址池）可以是具有地址范围的网络对象、定义子网的网络对象或包含所有地址的网络组池中。对于 FTD，“原始地址”池可以是定义包含池中所有地址的子网或网络组的网络对象。

Note 对于 ASA，定义“转换后的地址”池的网络组不能是定义子网的网络对象。

创建这些地址池时，请使用 Create or Edit ASA Network Objects and Network Groups use Create or Edit a Firepower Network Object or Network Groups 了解相关说明。创建或编辑 ASA 网络对象和网络组

出于以下程序的考虑，我们将私有地址池命名为 inside_pool，将公共地址池命名为 outside_pool。

步骤 1 在 CDO 导航栏中，点击**清单 (Inventory)**。

步骤 2 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

步骤 3 点击设备类型选项卡。

步骤 4 选择要为其创建 NAT 规则的设备。

步骤 5 点击右侧**管理 (Management)** 窗格中的 **NAT**。

步骤 6 点击  > **网络对象 NAT (Network Object NAT)**。

步骤 7 在第 1 部分**类型 (Type)** 中，选择**动态 (Dynamic)**，然后点击**继续 (Continue)**。

步骤 8 在第 2 部分**接口 (Interfaces)** 中，为源接口选择**内部**内部，为目标接口选择**外部**。点击**继续 (Continue)**。

步骤 9 在部分 3 数据包中，执行以下任务：

- 对于 Original Address，请点击**选择 (Choose)**，然后选择您在上述前提条件部分中创建的 **inside_pool** 网络对象（或网络组）。
- 对于 Translated Address，点击**选择 (Choose)**，然后选择您在上述前提条件部分中创建的 **outside_pool** 网络对象（或网络组）。

步骤 10 跳过第 4 节“高级”。

步骤 11 对于 FDM 管理的设备，在部分 5 (Name) 中，为 NAT 规则指定名称。

步骤 12 点击**保存 (Save)**。

步骤 13 立即 预览和部署所有设备的配置更改 您所做的更改，或等待并一次部署多个更改。

ASA 的已保存配置文件中的条目

这些是执行这些程序后将显示在 ASA 的已保存配置文件中的条目。

Note 这不适用于设备。FDM 管理

通过此程序创建的对象

```
object network outside_pool
    range 209.165.1.1 209.165.1.255
object network inside_pool
    range 10.1.1.1 10.1.1.255
```

此程序创建的 *NAT* 规则

```
object network inside_pool
nat (inside,outside) dynamic outside_pool
```

防止在遍历外部接口时转换某个范围的 IP 地址

使用案例

使用此两次 NAT 使用案例启用站点间 VPN。

策略

您将 IP 地址池转换为自身，以便网络上一个位置的 IP 地址到达另一个位置时保持不变。

创建两次 NAT 规则

Before you begin

创建定义要转换为自身的 IP 地址池的网络对象或网络组。对于 ASA，地址范围可以通过使用 IP 地址范围的网络对象、定义子网的网络对象或包含该范围内所有地址的网络组对象来定义。

创建网络对象或网络组时，请使用创建或编辑 ASA 网络对象和网络组获取说明。

在以下程序中，我们将调用网络对象或网络组，即站点间 PC 池。

步骤 1 在 CDO 导航栏中，点击**清单 (Inventory)**。

步骤 2 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

步骤 3 点击设备类型选项卡。

步骤 4 选择要为其创建 NAT 规则的设备。

步骤 5 点击右侧**管理 (Management)** 窗格中的 **NAT**。

步骤 6 点击  > **两次 NAT (Twice NAT)**。。

步骤 7 在第 1 部分中，**键入**选择**静态 (Static)**。点击**继续 (Continue)**。

步骤 8 在部分 2 中，为源接口选择内部，为目标接口选择外部。点击**继续 (Continue)**。

步骤 9 在第 3 部分**数据包**中，进行以下更改：

- 展开原始地址菜单，点击**Choose**，然后选择您在先决条件部分中创建的站点到站点 PC 池对象。
- 展开 Translated Address 菜单，点击 **Choose**，然后选择您在前提条件部分中创建的 Site-to-Site-PC-Pool 对象。

步骤 10 跳过第 4 节“高级”。

步骤 11 对于 FDM 管理的设备，在部分 5 (Name) 中，为 NAT 规则指定名称。

步骤 12 点击**保存 (Save)**。

步骤 13 为 ASA 创建一个加密映射。有关创建加密映射的详细信息，请参阅《CLI 手册 3：思科 ASA 系列 VPN CLI 配置指南》并查看 LAN 到 LAN IPsec VPN 一章。

步骤 14 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

ASA 的已保存配置文件中的条目

这些是执行这些程序后将显示在 ASA 的已保存配置文件中的条目。

Note 这不适用于设备。FDM 管理

通过此程序创建的对象

```
object network Site-to-Site-PC-Pool
range 10.10.2.0 10.10.2.255
```

此程序创建的 *NAT* 规则

```
nat (inside,outside) source static Site-to-Site-PC-Pool Site-to-Site-PC-Pool
```

在 CDO 中管理虚拟专用网络管理

虚拟专用网络 (VPN) 连接在使用公共网络（如互联网）的终端之间建立安全隧道。

本节适用于自适应安全设备 (ASA) 设备上的远程访问和站点间 VPN。它还介绍了用于在 ASA FTD 上构建和远程访问 VPN 连接的 SSL 标准。

CDO 支持以下几种类型的 VPN 配置：

- 站点间虚拟专用网络简介 ， 第 57 页
- 远程访问虚拟专用网络

站点间虚拟专用网络简介

站点间VPN隧道可连接不同地理位置的网络。您可以在托管设备之间以及托管设备与其他符合所有相关标准的思科或第三方对等体之间创建站点间的IPsec连接。这些对等体可以采用内部和外部IPv4和IPv6地址的任意组合。站点间隧道使用 Internet Protocol Security (IPsec) 协议套件或网络密钥交换版本 2 (IKEv2) 构建。建立 VPN 连接之后，本地网关后台的主机可通过安全 VPN 隧道连接至远程网关后台的主机。

VPN 拓扑

要创建一个新的站点间VPN拓扑，至少必须为其指定一个唯一名称，指定拓扑类型，选择用于IPsec IKEv1 和/或 IKEv2 的 IKE 版本。配置完毕后，可以将拓扑部署到 ASA。

IPsec 和 IKE 协议

在 CDO 中，站点间 VPN 是根据分配给 VPN 拓扑的 IKE 策略和 IPsec 建议配置的。策略和建议是定义站点到站点 VPN 的特性的参数集，例如用于在 IPsec 隧道中保护流量安全的安全协议和算法。可能需要多种策略类型来定义可以分配给 VPN 拓扑的完整配置映像。

身份验证 VPN 隧道

要对VPN连接进行身份验证，请在每个设备上拓扑中配置预共享密钥。预共享密钥允许在两个对等体之间共享安全密钥，该共享密钥在 IKE 身份验证阶段使用。

VPN 加密域

有两种方法可以定义 VPN 的加密域：路由型或策略型流量选择器。

- **策略型**：加密域设置为允许任何流量进入 IPSec 隧道。IPSec 本地和远程流量选择器会被设为 0.0.0.0。这意味着无论源/目标子网如何，路由到 IPSec 隧道的任何流量都会被加密。ASA 支持具有加密映射的策略型 VPN。
- **路由型**：加密域设置为仅加密源和目标的特定 IP 范围。它会创建一个虚拟 IPsec 接口，并且会加密和解密进入该接口的任何流量。ASA 通过使用虚拟隧道接口 (VTI) 来支持路由型 VPN。

关于外联网设备

您可以将非思科或非托管思科设备作为具有静态或动态IP地址的“外联网”设备添加到VPN拓扑。

- 非思科设备：不能使用 CDO 来创建配置以及将配置部署到非思科设备。
- 非托管思科设备：并非由贵公司管理的思科设备，例如，由您公司内的其他部门管理的网络中的分支，或者与服务提供商或合作伙伴的网络的连接。

相关信息：

- ASA 站点间 VPN 配置, on page 58
- 监控 ASA 站点间虚拟专用网络

ASA 站点间 VPN 配置

Cisco Defense Orchestrator (CDO) 支持自适应安全设备 (ASA) 设备上的站点间 VPN 功能：

- 支持 IPsec IKEv1 和 IKEv2 协议。
- 用于身份验证的自动或手动预共享密钥。
- IPv4 和 IPv6。支持内部和外部的所有组合。
- IPsec IKEv2 站点间 VPN 拓扑提供符合安全认证的配置设置。
- 静态和动态接口。
- 支持作为终端的外联网设备的静态或动态 IP 地址。

配置与动态寻址对等体的站点间 VPN 连接

如果其中一个对等体的 VPN 接口 IP 地址未知或接口从 DHCP 服务器获取其地址，CDO 允许您在对等体之间创建站点间 VPN 连接。预共享密钥、IKE 设置和 IPsec 配置与另一个对等体匹配的任何动态对等体都可以建立站点间 VPN 连接。

假设有两个对等体 A 和 B。静态对等体是其 VPN 接口为固定 IP 地址的设备，而动态对等体是其 VPN 接口为未知 IP 地址或具有临时 IP 地址的设备。

以下使用案例介绍了与动态寻址对等体建立安全站点间 VPN 连接的不同场景：

- A 是静态对等体，而 B 是动态对等体，反之亦然。
- A 是静态对等体，而 B 是具有来自 DHCP 服务器的已解析 IP 地址的动态对等体，反之亦然。
- A 是动态对等体，而 B 是具有静态或动态 IP 地址的外联网设备。
- A 是具有来自 DHCP 服务器的已解析 IP 地址的动态对等体，而 B 是具有静态或动态 IP 地址的外联网设备。

注释 如果使用自适应安全设备管理器 (ASDM) 等本地管理器更改了接口的 IP 地址，则 CDO 中该对等体的**配置状态 (Configuration Status)** 会显示“检测到冲突”(Conflict Detected)。当您解决“检测到冲突”状态时，其他对等体的**配置状态 (Configuration Status)** 会变成“未同步”(Not Synced) 状态。您必须将 CDO 配置部署到处于“未同步”(Not Synced) 状态的设备。

通常，连接必须由动态对等体发起，因为另一个对等体不知道动态对等体的 IP 地址。当远程对等体尝试建立连接时，另一个对等体会使用预共享密钥、IKE 设置和 IPsec 配置来验证连接。

由于只有在远程对等体发起连接之后才会建立VPN连接，因此在连接建立之前，系统会丢弃与允许流量通过 VPN 隧道的访问控制规则匹配的出站流量。这可确保数据不会在未采取适当加密和 VPN 保护措施的情况下离开您的网络。

注释 在以下情况下，无法配置站点间 VPN 连接：

如果设备有多个动态对等体连接。

- 考虑三台设备 A、B 和 C。
- 配置 A（静态对等体）和 B（动态对等体）之间的站点间 VPN 连接。
- 通过创建外联网设备来配置 A 和 C（动态对等体）之间的 VPN 连接。将 A 的静态 VPN 接口 IP 地址分配给外联网设备，并与 C 建立连接。

站点间 VPN 指南和限制

- CDO 不支持使用 crypto-acl 来设计 S2S VPN 需要关注的流量。它仅支持受保护的网络。
- 只要使用的是 IKE 端口 500/4500，或者有一些 PAT 转换处于活动状态，则无法在同一端口上配置站点间 VPN，因为无法在这些端口上启动服务。
- 不支持传输模式，仅支持隧道模式。IPsec 隧道模式对整个原始 IP 数据报进行加密，使其成为新 IP 数据包中的负载。当防火墙对出入位于防火墙后的主机的流量进行保护时，请使用隧道模式。在通过不可信网络（例如互联网）连接的两个防火墙（或其他安全网关）之间，通常采用隧道模式实施常规 IPsec。
- 对于此版本，仅支持包含一个或多个 VPN 隧道的 PTP 拓扑。点对点 (PTP) 部署在两个终端之间建立 VPN 隧道。

Virtual Tunnel Interface 准则

- VTI 只有在 IPsec 模式下才可配置。不支持在 ASA 上终止 GRE 隧道。
- 可以将动态或静态路由用于使用这种隧道接口的流量。
- VTI 的 MTU 将根据底层物理接口自动设置。但是，如果在启用 VTI 后更改物理接口 MTU，则您必须禁用并重新启用 VTI 才能使用新的 MTU 设置。
- 如果必须应用网络地址转换，则将 IKE 和 ESP 数据包封装在 UDP 报头中。
- 无论隧道中的数据流量如何，IKE 和 IPsec 安全关联都将不断重新生成密钥。这可确保 VTI 隧道始终处于活动状态。
- 隧道组名称必须与对等体作为其 IKEv1 或 IKEv2 身份发送的内容相符。
- 对于 LAN 间隧道组中的 IKEv1，仅当隧道身份验证方法为数字证书和/或对等体配置为使用积极模式时，才能使用非 IP 地址的名称。
- 只要加密映射中配置的对等体地址与 VTI 的隧道目的地址不同，VTI 和加密映射配置就可以在同一个物理接口上共存。
- 默认情况下，通过 VTI 的所有流量都经过加密。

- 默认情况下，VTI 接口的安全级别为 0。
- 可以在 VTI 接口上应用访问列表来控制通过 VTI 的流量。
- 仅 VTI 上支持 BGP。
- 如果 ASA 终结 IOS IKEv2 VTI 客户端，请禁用 IOS 上的配置交换请求，因为 ASA 无法为由 IOS VTI 客户端发起的 L2L 会话检索 mode-CFG 属性。
- 不支持 IPv6。

相关信息：

- 创建 ASA 站点间 VPN 隧道， 第 62 页
- VPN 中使用的加密和散列算法
- 从 NAT 豁免远程访问流量， 第 112 页

VPN 中使用的加密和散列算法

由于VPN隧道通常流经公共网络（最可能是互联网），因此您需要对连接进行加密以保护流量。可以使用 IKE 策略和 IPsec 提议定义要应用的加密和其他安全技术。

如果您的设备许可证允许应用较强的加密，则有大量的加密和散列算法以及Diffie-Hellman组供您选择。然而，通常情况下，应用于隧道的加密越强，系统性能越差。您要在安全性和性能之间实现平衡，在提供充分保护的同时不牺牲效率。

我们无法就选择哪些选项提供具体指导。如果您在大型公司或其他组织执行运营，可能已有需要满足的指定标准。如果没有，请花些时间研究各个选项。

下面的主题介绍了几个可用选项：

决定使用哪个加密算法

在决定用于 IKE 策略或 IPsec 提议的加密算法时，您的选择仅限于 VPN 中的设备所支持的算法。

对于 IKEv2，您可以配置多个加密算法。系统将按安全性从高到低的顺序对设置进行排序，并使用该顺序与对等体进行协商。对于 IKEv1，仅可以选择一个选项。

对于 IPsec 提议，该算法用于封装安全协议 (ESP)，该协议提供身份验证、加密和防重放服务。ESP 为 IP 协议类型 50。在 IKEv1 IPsec 提议中，算法名称以 ESP 为前缀。

如果设备许可证符合强加密要求，可以从以下加密算法中选择。如果不符合强加密要求，则只能选择 DES。

- AES-GCM -（仅限 IKEv2。）Galois/Counter 模式中的高级加密标准是提供机密性和数据源身份验证的分组加密操作模式，并且提供比 AES 更高的安全性。AES-GCM 提供三种不同的密钥强度：128 位、192 位和 256 位密钥。密钥越长，其提供的安全性就越高，但性能会随之降低。GCM 是支持 NSA Suite B 所需的 AES 模式。NSA Suite B 是一套加密算法，设备必须支持这套算法才能满足密码强度的联邦标准。

- AES-GMAC -（仅限 IKEv2 IPsec 提议。）高级加密标准 Galois 消息身份验证代码是仅提供数据源身份验证的分组加密操作模式。它是 AES-GCM 的一个变体，允许在不加密数据的情况下进行数据身份验证。AES-GMAC 提供三种不同的密钥强度：128 位、192 位和 256 位密钥。
- AES - 高级加密标准是一种对称密码算法，提供比 DES 更高的安全性，在计算上比 3DES 更高效。AES 提供三种不同的密钥强度：128 位、192 位和 256 位密钥。密钥越长，其提供的安全性就越高，但性能会随之降低。
- DES - 数据加密标准，使用 56 位密钥进行加密，是一种对称密钥块算法。如果您的许可证账户不符合导出控制要求，这将是您唯一的选择。此算法比 3DES 快且使用的系统资源更少，但安全性也较低。如果不需要很强的数据保密性，并且系统资源或速度存在问题，请选择 DES。
- 3DES - 三重 DES，使用 56 位密钥加密三次，比 DES 更加安全，因其使用不同密钥对每个数据块处理三次。不过，此算法比 DES 使用的系统资源更多且速度更慢。
- NULL - 空加密算法提供不加密的身份验证。这通常仅用于测试目的。

决定使用哪些散列算法

在 IKE 策略中，散列算法创建消息摘要，用于确保消息的完整性。在 IKEv2 中，散列算法分成两个选项，一个用于完整性算法，一个用于伪随机函数 (PRF)。

在 IPsec 提议中，散列算法由封装安全协议 (ESP) 用于身份验证。在 IKEv2 IPsec 提议中，这称为完整性散列。在 IKEv1 IPsec 提议中，算法名称以 ESP- 为前缀，并且还有 -HMAC 后缀（代表“散列方法身份验证代码”）。

对于 IKEv2，您可以配置多个散列算法。系统将按安全性从高到低的顺序对设置进行排序，并使用该顺序与对等体进行协商。对于 IKEv1，仅可以选择一个选项。

您可以选择以下散列算法：

- SHA （安全散列算法）- 生成 160 位摘要的标准 SHA (SHA-1)。SHA 抗暴力攻击的能力高于 MD5。但是，它也比 MD5 占用更多资源。对于需要最高级别安全性的实施，请使用 SHA 散列算法。
- 以下 SHA-2 选项更加安全，可用于 IKEv2 配置。如果要实施 NSA Suite B 加密规范，请选择以下选项之一。
  - SHA-256 - 指定具有 256 位摘要的安全散列算法 SHA-2。
  - SHA-384 - 指定具有 384 位摘要的安全散列算法 SHA-2。
  - SHA-512 - 指定具有 512 位摘要的安全散列算法 SHA-2。
- MD5（消息摘要 5）- 生成 128 位的摘要。MD5 能使用更少的处理时间实现比 SHA 更快的整体性能，但 MD5 被认为安全性低于 SHA。
- 空或无（NULL、ESP-NONE） -（仅限 IPsec 提议。）空散列算法；这通常仅用于测试目的。但是，如果选择 AES-GCM/GMAC 选项之一作为加密算法，则应选择空完整性算法。即使选择非空选项，这些加密标准也会忽略完整性散列。

决定要使用的 Diffie-Hellman 模数组

您可以使用以下 Diffie-Hellman 密钥导出算法生成 IPsec 安全关联 (SA) 密钥。每组具有不同的长度模数。模数更大则安全性越高，但需要更多的处理时间。两个对等体上必须具有一个匹配的模数组。

如果选择 AES 加密，要支持 AES 所需的大型密钥长度，应使用 Diffie-Hellman (DH) 组 5 或更高组。IKEv1 策略不支持下面列出的所有组。

要实施 NSA Suite B 加密规范，请使用 IKEv2 并选择椭圆曲线 Diffie-Hellman (ECDH) 的一个选项：19、20 或 21。使用 2048 位模数的椭圆曲线选项和组较少遭受 Logjam 等攻击。

对于 IKEv2，您可以配置多个组。系统将按安全性从高到低的顺序对设置进行排序，并使用该顺序与对等体进行协商。对于 IKEv1，仅可以选择一个选项。

- 2 - Diffie-Hellman 组 2：1024 位模幂算法 (MODP) 组。此选项不再是一种良好的保护措施。
- 5 - Diffie-Hellman 组 5：1536 位 MODP 组。曾经被认为可以良好地保护 128 位密钥，如今却不再是一种良好的保护措施。
- 14 - Diffie-Hellman 组 14：2048 位模幂算法 (MODP) 组。被认为可以良好地保护 192 位密钥。
- 19 - Diffie-Hellman 组 19：美国国家标准与技术研究所 (NIST) 256 位椭圆曲线取素数 (ECP) 组。
- 20 - Diffie-Hellman 组 20： NIST 384 位 ECP 组。
- 21 - Diffie-Hellman 组 21： NIST 521 位 ECP 组。
- 24 - Diffie-Hellman 组 24：带 256 位素数阶子组的 2048 位 MODP 组。我们不再建议采用此选项。

确定使用哪种身份验证方法

您可以使用以下方法对站点间 VPN 连接中的对等体进行身份验证。

预共享密钥

预共享密钥是在连接中的每个对等体上配置的加密密钥字符串。这些密钥由 IKE 在身份验证阶段使用。对于 IKEv1，您必须在每个对等体上配置相同的预共享密钥。对于 IKEv2，您可以在每个对等体上配置唯一密钥。

与证书相比，预共享密钥的扩展性相对逊色。如果需要配置大量的站点间VPN连接，请使用证书而非预共享密钥。

创建 ASA 站点间 VPN 隧道

使用以下程序在两个 ASA 或具有外联网设备的 ASA 之间创建站点间 VPN 隧道：

步骤 1 在导航窗格中，选择 **VPN** > **ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)**。

步骤 2 点击右上角的蓝色加号  ，然后点击**站点间 VPN (Site-to-Site VPN)** 和 ASA 标签。

步骤 3 在**配置名称 (Configuration Name)** 字段中，输入您创建的站点间 VPN 配置的名称。

步骤 4 选择以下选项之一，以便创建新的**策略型**或**路由型**站点间 VPN。

步骤 5 在**对等设备 (Peer Devices)** 部分中，执行以下操作：

a) **对等体 1 (Peer 1)**：选择 ASA 设备，然后点击**选择 (Select)**。

b) **对等体 2 (Peer 2)**：选择其他 ASA 设备，然后点击**选择 (Select)**。

外联网 (Extranet)：如果要在对等体 2 中选择外联网设备，请点击外联网滑块将其启用。

选择**静态 (Static)**，并指定 IP 地址，或为使用 DHCP 分配 IP 的外联网设备选择**动态 (Dynamic)**。**IP 地址 (IP Address)** 显示静态接口的 IP 地址或为动态接口**分配的 DHCP (DHCP Assigned)**。

c) 为终端设备选择 **VPN 访问接口** 。

d) （适用于路由型 VPN）选择控制 LAN 子网的 **LAN 接口**。您可以选择多个接口。

连接到所选 LAN 接口的网络将被添加到路由策略访问列表中。匹配路由策略访问列表的流量将由 VPN 隧道进行加密/解密。

e) 点击**添加网络 (Add Network)**，为参与的设备添加**受保护的网络 (Protected Networks)**。受保护的网络被定义为受此 VPN 终端保护的网络。

f) （可选且适用于策略型）选择 **NAT 免除 (NAT Exempt)** 以便从本地 VPN 访问接口的 NAT 策略中免除 VPN 流量。必须为单个对等体手动配置。如果不想将 NAT 规则应用于本地网络，请选择托管本地网络的接口。此选项仅在本地网络驻留在单个路由接口（而非网桥组成员）后时有用。如果本地网络位于多个路由接口或一个或多个网桥组成员之后，则必须手动创建 NAT 豁免规则。有关手动创建所需规则的信息，请参阅从 NAT 豁免 ASA 站点间 VPN 流量。

g) 点击**下一步**。

步骤 6 （适用于路由型）在**隧道详细信息 (Tunnel Details)** 中，一旦在上一步中配置了对等设备，就会自动填充 **VTI 地址 (VTI Address)** 字段。如有必要，您可以手动输入要用作新 VTI 的 IP 地址。

步骤 7 在 **IKE 设置 (IKE Settings)** 部分中，选择要在互联网密钥交换 (IKE) 协商期间使用的 IKE 版本，并指定隐私配置：有关 IKE 策略的详细信息，请参阅关于全局 IKE 策略。

根据用户所做的配置，CDO 会建议 IKE 设置。您可以继续使用建议的 IKE 配置设置，也可以定义新的配置设置。

注释 IKE 策略对设备是全局的，并应用于与其关联的所有 VPN 隧道。因此，添加或删除策略会影响此设备参与的所有 VPN 隧道。

a) 根据需要选择一个或两个 IKE 版本。

默认情况下，**IKEV 版本 2** 处于启用状态。

注释 不允许对路由型 VPN 启用两个 IKE 版本。

b) 点击**添加 IKEv2 策略 (Add IKEv2 Policy)**，然后选择 IKEv2 策略

注释 点击 **创建新的 IKEv2 策略** 以创建新的 IKEv2 策略。有关创建新 IKEv2 策略的详细信息，请参阅管理 IKEv2 策略。要删除现有 IKEv2 策略，请将鼠标悬停在所选策略上，然后点击 x 图标。

c) 输入参与设备的**预共享密钥**。预共享密钥是在连接中的每个对等体上配置的加密密钥字符串。IKE在身份验证阶段使用这些密钥。

(IKEv2) **对等体 1 预共享密钥、对等体 2 预共享密钥**：对于 IKEv2，您可以在每个对等体上配置唯一的密钥。输入**预共享密钥 (Pre-shared Key)**。您可以点击显示按钮，并为对等体输入适当的预共享。该密钥可以有 1 至 127 个字母数字字符。下表介绍了两个对等体的预共享密钥的用途。

	本地预共享密钥	远程对等预共享密钥
对等体 1	对等体 1 预共享密钥	对等体 2 预共享密钥
对等体 2	对等体 2 预共享密钥	对等体 1 预共享密钥

d) 点击 **IKE 版本 1** 以启用它。

e) 点击**添加 IKEv1 策略 (Add IKEv1 Policy)**，然后选择 IKEv1 策略。点击 **创建新的 IKEv1 策略** 以创建新的 IKEv1 策略。有关创建新 IKEv1 策略的详细信息，请参阅 管理 IKEv1 策略。要删除现有 IKEv1 策略，请将鼠标悬停在所选策略上，然后点击 x 图标。

f) (IKEv1) **预共享密钥**：对于 IKEv1，您必须在每个对等体上配置相同的预共享密钥。该密钥可以有 1 至 127 个字母数字字符。在此场景中，对等体 1 和对等体 2 使用相同的预共享密钥加密和解密数据。

g) 点击**下一步**。

步骤 8 在 **IPSec 设置 (IPSec Settings)** 部分，根据用户所做的配置，CDO 会建议 IKEv2 提议。您可以继续使用建议的 IKE 配置设置，也可以定义新的配置设置。有关 IPSec 设置的详细信息，请参阅配置 IPsec 提议。

a) 点击**+ IKEv2 提议 (+ IKEv2 Proposals)** 以选择 IPSec 配置。相应的 IKEV 提议是否可用，具体取决于在 **IKE 设置** 步骤中所做的选择。要删除现有的 IKEv2 提议，请将鼠标悬停在所选提议上，然后点击 x 图标。

注释 点击**创建新的 IKEv2 提议 (Create New IKEv2 Proposals)** 以创建新的 IKEv2 提议。有关创建新 IKEv2 策略的详细信息，请参阅关于 IPSec 提议。

b) 选择**适用于完全向前保密的 Diffie-Hellman 组 (Diffie-Hellman Group for Perfect Forward Secrecy)**。有关详细信息，请参阅VPN 中使用的加密和散列算法，第 60 页

c) 点击**下一步**。

步骤 9 在**完成**部分中，请阅读配置，并在您对配置满意时继续操作，然后点击**提交 (Submit)**。

您将被定向到“VPN 隧道” (VPN Tunnels)页面，该页面显示新配置的站点间 VPN 隧道。这些更改已暂存，并且必须手动部署。系统会创建路由策略，以便通过 VTI 隧道在设备之间自动路由 VTI 流量。要查看此策略，请从**清单 (Inventory)** 页面中选择设备，然后选择**配置 (Configuration)** > **差异 (Diff)**。

请参阅部署使用 CDO GUI 进行的配置更改部分，在与新隧道关联的设备上部署站点间 VPN 配置。

删除 CDO 站点间 VPN 隧道

步骤 1 在导航栏上，选择 **VPN**> **ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)**。

步骤 2 选择要删除的所需站点间 VPN 隧道。

步骤 3 在**操作 (Actions)** 窗格中，点击**删除 (Delete)**。

所选站点间 VPN 隧道将被删除。

使站点间 VPN 流量豁免 NAT

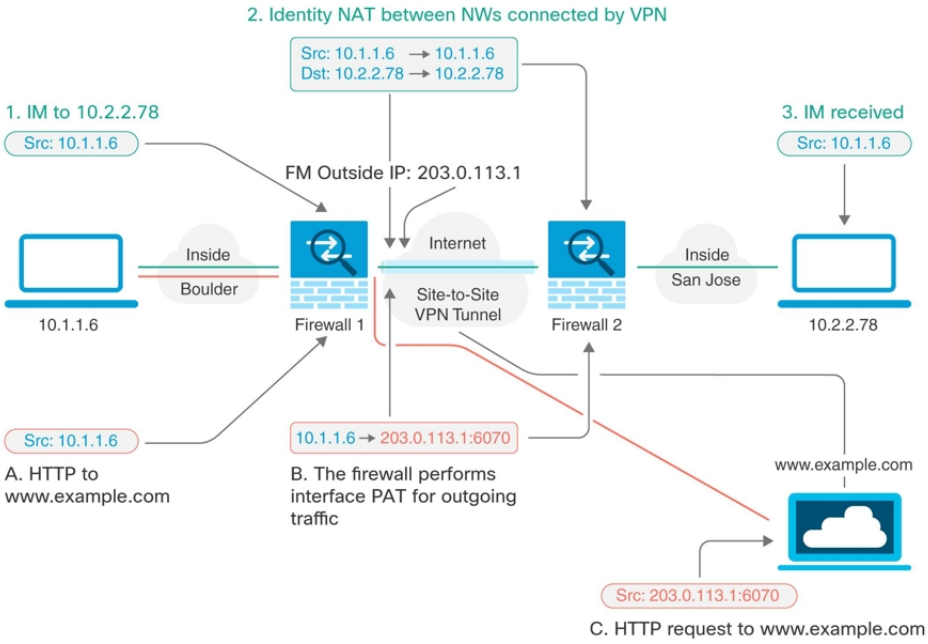
当您在某个接口上定义了站点间 VPN 连接并且还对该接口实施了 NAT 规则时，可以选择使该 VPN 上的流量豁免 NAT 规则。如果 VPN 连接的远端可以处理您的内部地址，则可能要执行此操作。

创建 VPN 连接时，可以选择 **NAT 豁免**选项自动创建 NAT 豁免规则。不过，此操作仅在通过单个路由接口（而非网桥组成员）连接本地受保护网络时才奏效。相反，如果该连接中的本地网络位于两个或多个路由接口之后或者一个或多个网桥组成员之后，则需要手动配置 NAT 豁免规则。

要使 VPN 流量豁免 NAT 规则，需要为目的是远程网络时的本地流量创建身份手动 NAT 规则。然后，将NAT应用于目的是其他网络（例如互联网）时的流量。如果本地网络有多个接口，请为每个接口分别创建规则。也可以考虑以下建议：

- 如果连接中有多个本地网络，请创建一个网络对象组用于容纳定义这些网络的对象。
- 如果 VPN 中同时包括 IPv4 和 IPv6 网络，请为其各创建一个单独的身份 NAT 规则。

下例显示连接博尔德办公室和圣荷西办公室的站点间隧道。对于要发送到互联网的流量（例如，从博尔德办公室中的 10.1.1.6 到 www.example.com），需要利用 NAT 提供的公用 IP 地址访问互联网。以下示例使用接口端口地址转换 (PAT) 规则。然而，对于要穿过 VPN 隧道的流量（例如，从博尔德办公室中的 10.1.1.6 到圣荷西办公室中的 10.2.2.78），您不想执行 NAT；您需要通过创建身份 NAT 规则来豁免此流量。身份 NAT 将地址转换为其相同的地址。



以下示例说明 Firewall1（博尔德办公室）的配置。该示例假定内部接口是网桥组，因此需要为每个成员接口编写规则。如果有一个或多个路由内部接口，其过程相同。

Note 此示例假定只包括 IPv4 网络。如果该 VPN 还包括 IPv6 网络，请为 IPv6 创建并行规则。请注意，由于无法实施 IPv6 接口 PAT，因此需要使用唯一 IPv6 地址创建主机对象用于 PAT。

步骤 1 创建对象来定义各种网络。

a. 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

b. 点击蓝色加号按钮  以创建新的对象。

c. 点击 **ASA** > **网络**。

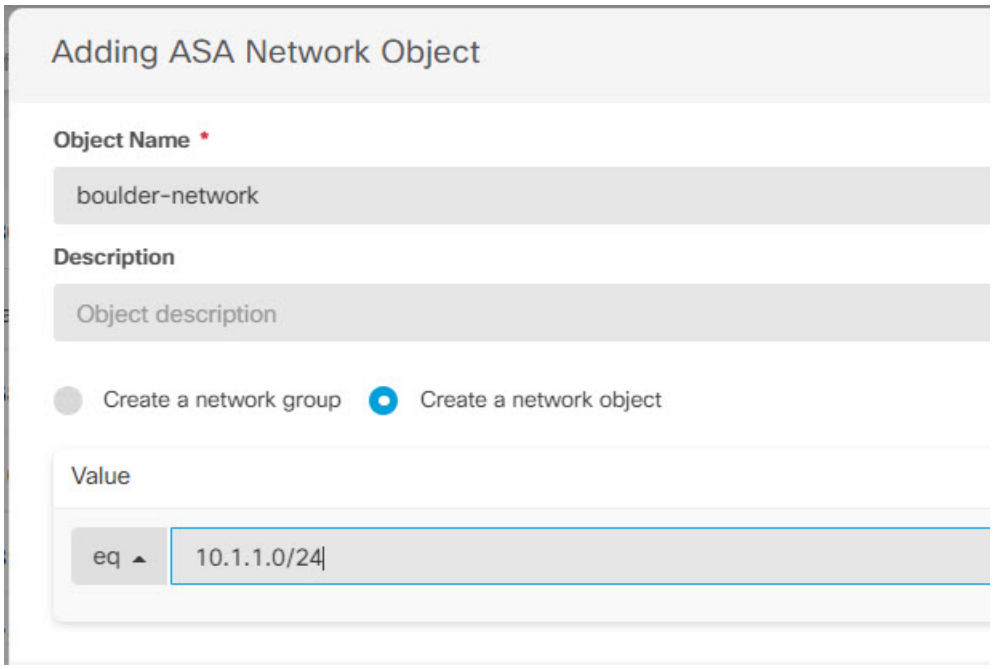
d. 找到博尔德办公室内部网络。

e. 输入对象名称（例如，boulder-network）。

f. 选择 **创建网络对象**。

g. 在“值”部分：

- 选择 **eq** 并输入以 CIDR 表示法表示的单个 IP 地址或子网地址。
- 选择 **范围** 并输入 IP 地址范围。例如，输入网络地址 10.1.1.0/24。



h. 点击**添加 (Add)**。

i. 点击蓝色加号按钮  以创建新的对象。

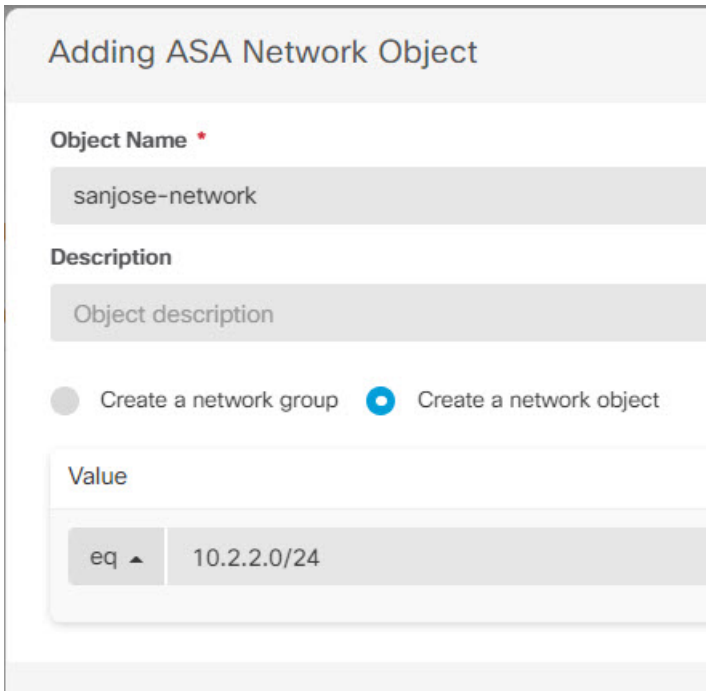
j. 定义内部圣荷西办公室网络。

k. 输入对象名称（例如，san-jose）。

l. 选择 **创建网络对象**。

m. 在“值”部分：

- 选择 **eq** 并输入以 CIDR 表示法表示的单个 IP 地址或子网地址。
- 选择 **范围** 并输入 IP 地址范围。例如，输入网络地址 10.1.1.0/24。



n. 点击**添加 (Add)**。

步骤 2 在 Firewall1（博尔德办公室）上，为博尔德办公室网络配置经过 VPN 连接到圣荷西办公室时的手动身份 NAT。

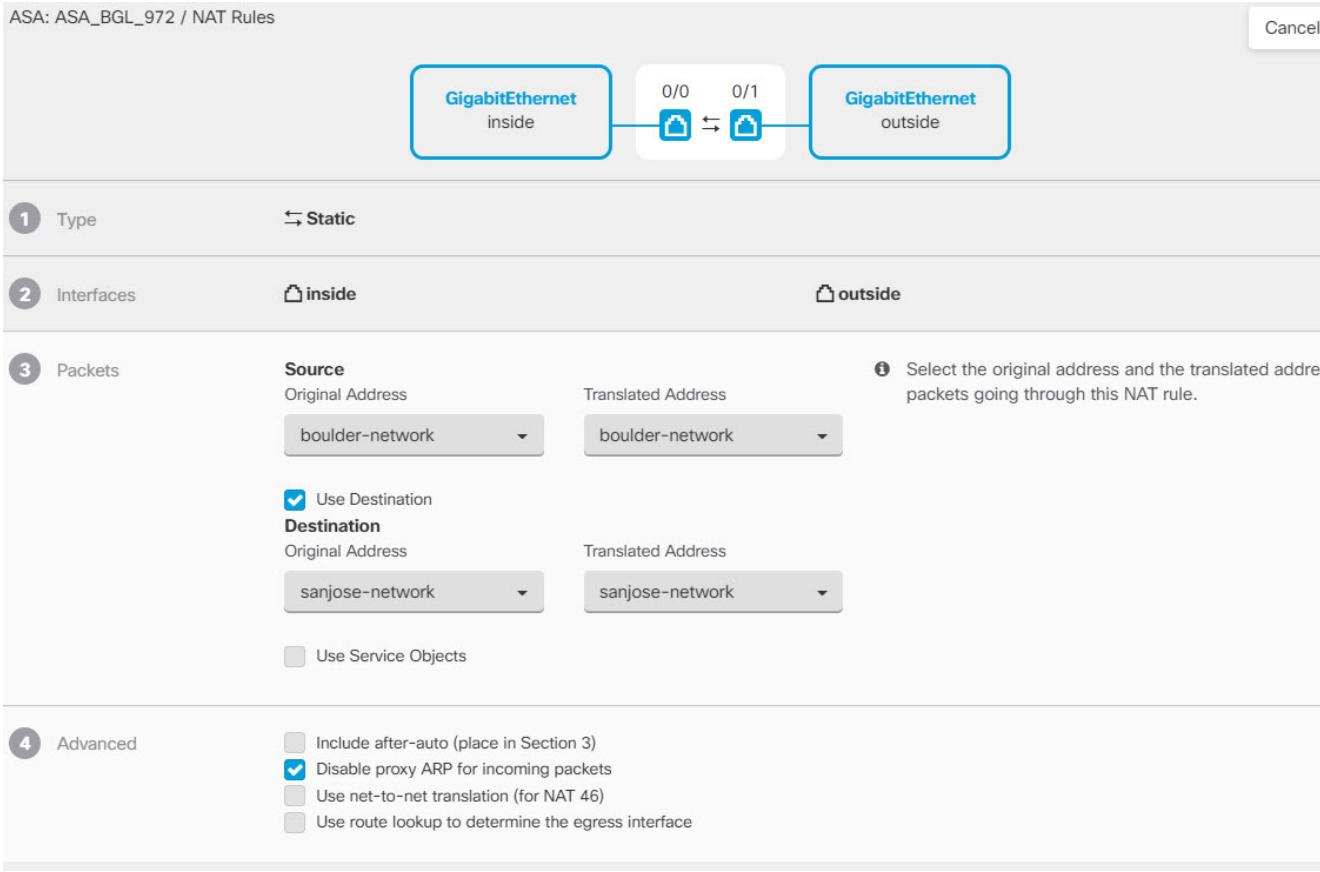
a. 在 CDO 导航栏中，点击**清单 (Inventory)**。

b. 使用过滤器查找要为其创建 NAT 规则的设备。

c. 在详细信息面板的管理区域中，点击 **NAT** NAT。

d. 点击 + > **两次 NAT**。

- 在第 1 部分中，选择**静态 (Static)**。点击**继续**。
- 在部分 2 中，选择**源接口 (Source Interface)** = **inside** 和**目标接口 (Destination Interface)** = **outside**。点击**继续**。
- 在第 3 部分中，选择**原始源地址 (Source Original Address)** = 'boulder-network' 和 **转换后的源地址 (Source Translated Address)** = 'boulder-network'。
- 选择 **使用目的**。
- 选择**原始目标地址 (Destination Original Address)** = 'sanjose-network' 和**转换后的源地址 (Source Translated Address)** = 'sanjose-network'。**注意：**由于您不需要转换目的地址，因此需要通过为原始目的地址和转换后的目的地址指定相同的地址，从而为其配置身份 NAT。将所有端口字段留空。此规则为源和目标配置身份 NAT。



- 选择为传入数据包禁用代理 **ARP (Disable proxy ARP for incoming packets)**。
- 点击保存 **(Save)**。
- 重复此过程，为每个其他内部接口创建相应规则。

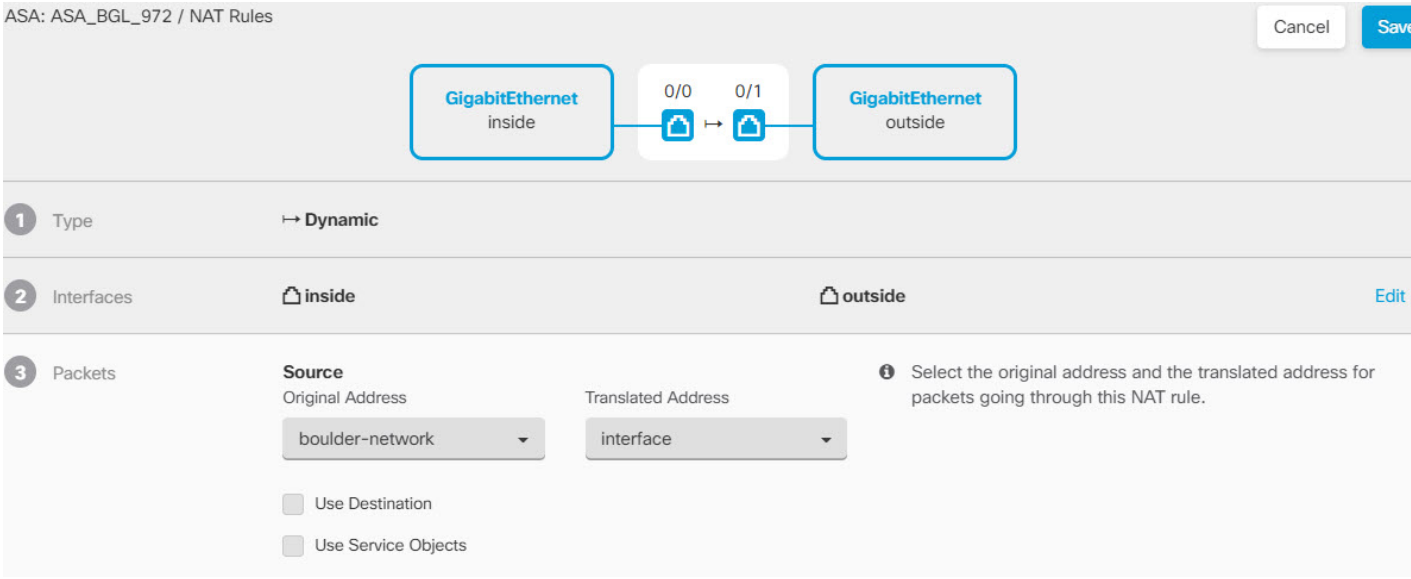
步骤 3 在 Firewall1（博尔德办公室）上，为内部博尔德办公室网络配置接入互联网时的手动动态接口 PAT。**注意：**内部接口可能已经配置了将所有 IPv4 流量包括在内的动态接口 PAT 规则，因为初始配置过程中会默认创建这些规则。不过，为完整起见，此处仍显示了这些配置。完成这些步骤之前，请检查是否已经存在将内部接口和网络包括在内的规则，如有则跳过此步骤。

a. 点击 + > **两次 NAT**。

b. 在第 1 部分中，选择**动态 (Dynamic)**。点击**继续**。

c. 在部分 2 中，选择**源接口 (Source Interface)** = **inside** 和**目标接口 (Destination Interface)** = **outside**。点击**继续**。

d. 在第 3 部分中，选择**原始源地址 (Source Original Address)** = 'boulder-network' 和**转换后的源地址 (Source Translated Address)** = 'interface'。



e. 点击**保存 (Save)**。

f. 重复此过程，为每个其他内部接口创建相应规则。

步骤 4 将配置更改部署到 CDO。有关详细信息，请参阅部署使用 CDO GUI 进行的配置更改, on page 163。

步骤 5 如果您也管理着 Firewall2（圣荷西办公室），您可以为该设备配置类似的规则。

- 当目标是 boulder-network 时，手动身份 NAT 规则将用于 'sanjose-network'。为 Firewall2 内部和外部网络创建新的接口对象。
- 当目标是“任何”时，手动动态接口 PAT 规则将用于 'sanjose-network'。

关于全局 IKE 策略

互联网密钥交换 (IKE) 是用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA) 的密钥管理协议。

IKE 协商包含两个阶段。第 1 阶段协商两个 IKE 对等体之间的安全关联，使对等体能够在第 2 阶段中安全通信。在第 2 阶段协商期间，IKE 为其他应用建立 SA，例如 IPsec。两个阶段在协商连接时均使用提议。IKE 提议是一组两个对等体用于保护其之间的协商的算法。在各对等体商定公共（共享）IKE 策略后，即开始 IKE 协商。此策略声明哪些安全参数用于保护后续 IKE 协商。

IKE 策略对象为这些协商定义 IKE 提议。您启用的对象是对等体协商 VPN 连接时使用的对象：不能为每个连接指定不同的 IKE 策略。每个对象的相对优先级确定首先尝试这些策略中的哪一个，数字越小优先级越高。如果协商无法找到两个对等体全都支持的策略，则不建立连接。

要定义全局 IKE 策略，需要为每个 IKE 版本选择启用哪些对象。如果预定义的对象不能满足您的要求，请创建新的策略来执行您的安全策略。

以下步骤说明如何通过“对象”(Objects) 页面配置全局策略。在编辑 VPN 连接时，您还可以点击 IKE 策略设置的编辑，来启用、禁用和创建策略。

以下主题介绍如何为每个 IKE 策略版本配置 IPsec 提议：

- 管理 IKEv1 策略
- 管理 IKEv2 策略

管理 IKEv1 策略

关于 IKEv1 策略

互联网密钥交换 (IKE) 版本 1 策略对象包含定义 VPN 连接时 IKEv1 策略所需的参数。IKE 是一种密钥管理协议，有助于管理基于 IPsec 的通信。它用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA)。

预定义的 IKEv1 策略有多个。如果哪个符合您的需求，只需点击状态开关便可启用它们。您还可以创建新策略来实施其他安全设置组合。但您无法编辑或删除系统定义的对象。

Related Topics

创建 IKEv1 策略，第 71 页

创建 IKEv1 策略

互联网密钥交换 (IKE) 版本 1 策略对象包含定义 VPN 连接时 IKEv1 策略所需的参数。IKE 是一种密钥管理协议，有助于管理基于 IPsec 的通信。它用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA)。

预定义的 IKEv1 策略有多个。如果哪个符合您的需求，只需点击状态开关便可启用它们。您还可以创建新策略来实施其他安全设置组合。但您无法编辑或删除系统定义的对象。

以下程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。您还可以点击对象列表中所示的**创建新 IKE 策略 (Create New IKEv1 Policy)** 链接，以便在站点间 VPN 连接中编辑 IKEv1 设置时创建 IKEv1 策略对象。

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 执行以下操作之一：

- 点击蓝色加号按钮  ，然后选择**FDM** > **IKEv1 策略 (IKEv1 Policy)** 以创建新的 IKEv1 策略。
- 在对象页面中，选择要编辑的 IKEv1 策略，然后点击右侧“操作”(Actions) 窗格中的**编辑 (Edit)**。

步骤 3 输入**对象名称**，最多 128 个字符。

步骤 4 配置 IKEv1 属性。

- **优先级** - IKE 策略的相对优先级，从 1 到 65,535。当尝试查找常见安全关联 (SA) 时，优先级可确定两个协商对等体比较的 IKE 策略顺序。如果远程 IPsec 对等体不支持在您的最高优先级策略中选定的参数，它会尝试使用下一个优先级中定义的参数。数值越低，优先级越高。

- **加密** - 用于建立第 1 阶段安全关联 (SA)（用于保护第 2 阶段协商）的加密算法。有关选项的说明，请参阅“决定使用哪种加密算法”。
- **Diffie-Hellman 组 (Diffie-Hellman Group)** - 用于在两个 IPsec 对等体之间派生共享密钥而不将其相互传输的 Diffie-Hellman 组。模数更大则安全性越高，但需要更多的处理时间。两个对等体必须具有匹配的模数组。有关选项的解释，请看“决定要使用的 Diffie-Hellman 模数组”。
- **生命周期 (Lifetime)** - 安全关联 (SA) 的生命周期（以秒为单位）范围为 120 到 2147483647，也可以将其留空。当超过生命周期时，SA 到期且必须在两个对等体之间重新协商。通常，生命周期越短（某种程度上），IKE 协商越安全。但是，生命周期越长，将来设置 IPsec 安全关联的速度比生命周期较短时更快。默认值为 86400。要指定无限生命周期，请不要输入任何值（将此字段留空）。
- **身份验证 (Authentication)** - 在两个对等体之间使用的身份验证方法。关于更多信息，请参阅 确定使用哪种身份验证方法。
  - **预共享密钥** - 使用在每个设备上定义的预共享密钥。在身份验证阶段，此类密钥允许密钥在两个对等体之间共享并由 IKE 使用。如果未使用同一预共享密钥配置对等体，则无法建立 IKE SA。
  - **证书 (Certificate)** - 使用对等体的设备身份证书来识别彼此。必须通过在证书颁发机构中注册每个对等体来获取这些证书。还须上传用于签署每个对等体的身份证书的受信任 CA 根证书和中间 CA 证书。对等体可以注册到相同或不同的 CA 中。对于任一对等体，都不能使用自签证书。
- **散列** - 用于创建消息摘要的散列算法，以确保消息的完整性。有关选项的说明，请参阅决定要使用的 Diffie-Hellman 模数组。

步骤 5 点击 **Add**。

管理 IKEv2 策略

关于 IKEv2 策略

互联网密钥交换 (IKE) 版本 2 策略对象包含定义 VPN 连接时 IKEv2 策略所需的参数。IKE 是一种密钥管理协议，有助于管理基于 IPsec 的通信。它用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA)。

预定义的 IKEv2 策略有多个。如果哪个符合您的需求，只需点击状态开关便可启用它们。您还可以创建新策略来实施其他安全设置组合。但您无法编辑或删除系统定义的对象。

Related Topics

创建 IKEv2 策略 , 第 72 页

创建 IKEv2 策略

互联网密钥交换 (IKE) 版本 2 策略对象包含定义 VPN 连接时 IKEv2 策略所需的参数。IKE 是一种密钥管理协议，有助于管理基于 IPsec 的通信。它用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA)。

预定义的 IKEv2 策略有多个。如果哪个符合您的需求，只需点击状态开关便可启用它们。您还可以创建新策略来实施其他安全设置组合。但您无法编辑或删除系统定义的对象。

以下程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。您还可以点击对象列表中所示的 **创建新的 IKE 策略** 链接，以便在站点间 VPN 连接中编辑 IKEv1 设置时创建 IKEv1 策略对象。

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 执行以下操作之一：

- 点击蓝色加号按钮  ，然后选择 **FDM** > **IKEv2 策略 (IKEv2 Policy)** 以创建新的 IKEv2 策略。
- 在对象页面中，选择要编辑的 IKEv2 策略，然后点击右侧“操作”(Actions) 窗格中的**编辑 (Edit)**。

步骤 3 输入**对象名称 (object name)**，最多 128 个字符。

步骤 4 配置 IKEv2 属性。

- **优先级** - IKE 策略的相对优先级，从 1 到 65,535。当尝试查找常见安全关联 (SA) 时，优先级可确定两个协商对等体比较的 IKE 策略顺序。如果远程 IPsec 对等体不支持在您的最高优先级策略中选定的参数，它会尝试使用下一个优先级中定义的参数。数值越低，优先级越高。
- **状态** - IKE 策略是启用还是禁用状态。点击开关以更改状态。在 IKE 协商期间仅使用启用的策略。
- **加密 (Encryption)** - 用于建立第 1 阶段安全关联 (SA)（用于保护第 2 阶段协商）的加密算法。选择要允许的所有算法，但不能在同一策略中同时包括混合模式 (AES-GCM) 和正常模式选项。（正常模式要求选择完整性散列，而混合模式禁止选择单独的完整性散列。) 系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅决定决定使用哪个加密算法。
- **Diffie-Hellman 组 (Diffie-Hellman Group)** - 用于在两个 IPsec 对等体之间派生共享密钥而不将其相互传输的 Diffie-Hellman 组。模数更大则安全性越高，但需要更多的处理时间。两个对等体必须具有匹配的模数组。选择要允许的所有算法。系统与对等体协商，从最强到最弱组，直到达成匹配。有关选项的解释，请参阅决定要使用的 Diffie-Hellman 模数组。
- **完整性散列 (Integrity Hash)** - 用于创建消息摘要的散列算法的完整性部分，用于确保消息完整性。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。完整性散列不与 AES-GCM 加密选项一起使用。有关选项的说明，请参阅 决定使用哪些散列算法。
- **伪随机函数 (PRF) 散列 (Pseudo-Random Function [PRF] Hash)** - 散列算法中用作派生 IKEv2 隧道加密所要求的密钥内容和散列运算的算法的伪随机函数 (PRF) 部分。在 IKEv1 中，完整性和 PRF 算法不分开，但在 IKEv2 中，可以为这些元素指定不同的算法。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅决定使用哪些散列算法。
- **生命周期 (Lifetime)** - 安全关联 (SA) 的生命周期（以秒为单位）范围为 120 到 2147483647，也可以将其留空。当超过生命周期时，SA 到期且必须在两个对等体之间重新协商。通常，生命周期越短（某种程度上），IKE 协商越安全。但是，生命周期越长，将来设置 IPsec 安全关联的速度比生命周期较短时更快。默认值为 86400。要指定无限生命周期，请不要输入任何值（将此字段留空）。

步骤 5 点击 **Add**。

关于 IPSec 提议

IPsec 是设置 VPN 的最安全方法之一。IPsec 在 IP 数据包级别提供数据加密，提供一种基于标准的强大的安全解决方案。使用 IPsec，数据通过隧道在公共网络上传输。隧道是两个对等体之间安全的逻辑通信路径。进入 IPsec 隧道的流量由称为转换集的安全协议和算法组合保护。在 IPsec 安全关联 (SA) 协商期间，对等体搜索在两个对等体处相同的转换集。

根据 IKE 版本（IKEv1 或 IKEv2），存在不同的 IPsec 提议对象：

- 当创建 IKEv1 IPsec 提议时，可以选择 IPsec 运行的模式，并定义所需的加密和身份验证类型。您可以为算法选择单一选项。如果要在 VPN 中支持多个组合，请创建和选择多个 IKEv1 IPsec 提议对象。
- 当创建 IKEv2 IPsec 提议时，可以选择 VPN 中允许的所有加密和散列算法。系统将按安全性从高到低的顺序对设置进行排序，并与对等体进行协商，直到找到匹配。利用这种排序，您可以发送单个提议来传达所有允许的组合，而无需像 IKEv1 一样逐一发送每个允许的组合。

IKEv1 和 IKEv2 IPsec 提议都使用封装安全协议 (ESP)。它可以提供身份验证、加密和反重播服务。ESP 为 IP 协议类型 50。

Note 我们建议对 IPsec 隧道使用加密和身份验证。

以下主题介绍如何为每个 IKE 版本配置 IPsec 提议：

- 管理 IKEv1 IPsec 提议对象
- 管理 IKEv2 IPsec 提议对象

管理 IKEv1 IPsec 提议对象

IPsec 提议对象配置 IKE 第 2 阶段协商期间使用的 IPsec 提议。IPsec 提议定义在 IPsec 隧道中保护流量的安全协议和算法的组合。IKEv1 和 IKEv2 有单独的对象。目前， Cisco Defense Orchestrator (CDO) 支持 IKEv1 IPsec 提议对象。

IKEv1 和 IKEv2 IPsec 提议都使用封装安全协议 (ESP)。它可以提供身份验证、加密和反重播服务。ESP 为 IP 协议类型 50。

Note 我们建议对 IPsec 隧道使用加密和身份验证。

Related Topics

创建 IKEv1 IPsec 提议对象 ， 第 74 页

创建 *IKEv1 IPsec* 提议对象

IPsec 提议对象配置 IKE 第 2 阶段协商期间使用的 IPsec 提议。IPsec 提议定义在 IPsec 隧道中保护流量的安全协议和算法的组合。IKEv1 和 IKEv2 有单独的对象。目前， Cisco Defense Orchestrator (CDO) 支持 IKEv1 IPsec 提议对象。

IKEv1 和 IKEv2 IPsec 提议都使用封装安全协议 (ESP)。它可以提供身份验证、加密和反重播服务。ESP 为 IP 协议类型 50。

Note 我们建议对 IPsec 隧道使用加密和身份验证。

有几个预定义的 IKEv1 IPsec 提议。您也可以创建新的提议，用于实施安全设置的其他组合。但您无法编辑或删除系统定义的对象。

以下程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。此外，也可以在编辑站点间 VPN 连接中的 IKEv1 IPsec 设置时，点击对象列表中所示的**创建新 IKEv1 提议 (Create New IKEv1 Proposal)** 链接来创建 IKEv1 IPsec 提议对象。

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 执行以下操作之一：

- 点击蓝色加号按钮  ，然后选择 **FDM > IKEv1 IPsec 提议 (IKEv1 IPsec Proposal)** 以创建新对象。
- 在对象页面中，选择要编辑的 IPsec 方案，然后点击右侧“操作”(Actions) 窗格中的**编辑 (Edit)**。

步骤 3 为新对象输入**对象名称**。

步骤 4 选择 IKEv1 IPsec 提议对象的运行模式。

- **隧道**模式会封装整个 IP 数据包。IPSec 报头被添加到原始 IP 报头和新的 IP 报头之间。这是默认值。当防火墙对出入位于防火墙后的主机的流量进行保护时，请使用隧道模式。在通过不可信网络（例如互联网）连接的两个防火墙（或其他安全网关）之间，通常采用隧道模式实施常规 IPSec。
- **传输**模式只封装 IP 数据包的上层协议。IPSec 报头被插入到 IP 报头和上层协议报头（例如 TCP）之间。传输模式要求源和目的主机都支持 IPSec，并且只有在隧道的目的对等体是 IP 数据包的最终目的时才可使用。通常只有在保护第 2 层或第 3 层隧道协议（例如 GRE、L2TP 和 DLSW）时，才会使用传输模式。

步骤 5 选择**加密 (Encryption)**提议的（封装安全协议加密）算法。有关选项的说明，请参阅 决定使用哪个加密算法。

步骤 6 选择要用于身份验证的 **ESP 散列 (ESP Hash)** 或完整性算法。有关选项的说明，请参阅决定使用哪些散列算法。

步骤 7 点击 **Add**。

管理 IKEv2 IPsec 提议对象

IPsec 提议对象配置 IKE 第 2 阶段协商期间使用的 IPsec 提议。IPsec 提议定义在 IPsec 隧道中保护流量的安全协议和算法的组合。

当创建 IKEv2 IPsec 提议时，可以选择 VPN 中允许的所有加密和散列算法。系统将按安全性从高到低的顺序对设置进行排序，并与对等体进行协商，直到找到匹配。利用这种排序，您可以发送单个提议来传达所有允许的组合，而无需像 IKEv1 一样逐一发送每个允许的组合。

Related Topics

创建或编辑 IKEv2 IPsec 提议对象 ， 第 76 页

创建或编辑 *IKEv2 IPsec* 提议对象

有几个预定义的IKEv2 IPsec提议。您也可以创建新的提议，用于实施安全设置的其他组合。但您无法编辑或删除系统定义的对象。

以下程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。此外，也可以在编辑 VPN 连接中的 IKEv2 IPsec 设置时，点击对象列表中所示的创建新 IPsec 提议链接来创建 IKEv2 IPsec 提议对象。

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 执行以下操作之一：

- 点击蓝色加号按钮  ，然后选择 **FDM** > **IKEv2 IPsec 提议 (IKEv2 IPsec Proposal)** 以创建新对象。
- 在对象页面中，选择要编辑的 IPsec 方案，然后点击右侧“操作”(Actions) 窗格中的**编辑 (Edit)**。

步骤 3 为新对象输入**对象名称**。

步骤 4 配置 IKEv2 IPsec 方案对象：

- **加密 (Encryption)** - 此提议的封装安全协议 (ESP) 加密算法。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅决定决定使用哪个加密算法.
- **完整性散列 (Integrity Hash)** - 要用于身份验证的散列或完整性算法。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅决定使用哪些散列算法。

步骤 5 点击**添加 (Add)**。

监控 ASA 站点间虚拟专用网络

通过 CDO，您可以监控已载入的 ASA 设备上的现有站点间 VPN 配置。它不允许您修改或删除站点间配置。

检查站点间 VPN 隧道连接

使用 Check Connectivity 按钮触发对隧道的实时连接检查，以确定隧道当前处于活动状态还是空闲状态。搜索和过滤器站点间 VPN 隧道, on page 79除非您点击“按需连接检查”按钮，否则将每小时检查一次所有已载入设备上可用的所有隧道。

Note

- CDO 在 ASA FTD 上运行此连接检查命令，以确定隧道处于活动状态还是空闲状态：

```
show vpn-sessiondb l2l sort ipaddress
```

- 建模 ASA 设备将始终显示为空闲。

要从 VPN 页面检查隧道连接，请执行以下操作：

步骤 1 在主导航栏中，点击 VPN > ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)。

步骤 2 搜索并过滤站点间 VPN 隧道的隧道列表，然后选择该列表。搜索和过滤器站点间 VPN 隧道, on page 79

步骤 3 在右侧的操作窗格中，点击检查连接。

确定 VPN 问题

CDO 可以识别 ASA FTD 上的 VPN 问题。（此功能尚不适用于 AWS VPC 站点间 VPN 隧道。）本文将介绍以下内容：

- 查找缺少对等体的 VPN 隧道
- 查找存在加密密钥问题的 VPN 对等体
- 查找为隧道定义的不完整或配置错误的访问列表
- 查找隧道配置中的问题

解决隧道配置问题, on page 78

查找缺少对等体的 *VPN* 隧道

“缺少 IP 对等体”情况在 ASA 设备上比设备上更可能发生。FDM 管理

步骤 1 在 CDO 导航窗格中，点击 **VPN** > **ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)** 以打开 VPN 页面。

步骤 2 选择**表视图 (Table View)**。

步骤 3 通过点击过滤器图标 打开过滤器面板。

步骤 4 检查检测到的问题。

步骤 5 选择每个报告问题的设备，然后查看右侧的“对等体”窗格。系统将列出一个对等体名称。CDO 报告另一个对等体名称为“[缺少对等体 IP.]”。

查找存在加密密钥问题的 *VPN* 对等体

使用此方法查找存在加密密钥问题的 VPN 对等体，例如：

- IKEv1 或 IKEv2 密钥无效、缺失或不匹配
- 过时或低加密隧道

步骤 1 在 CDO 导航栏中，点击 **VPN** > **ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)** 以打开 VPN 页面。

步骤 2 选择**表视图 (Table View)**。

步骤 3 通过点击过滤器图标 打开过滤器面板。

步骤 4 选择每个报告问题的设备，然后查看右侧的“对等体”窗格。⚠对等体信息将显示两个对等体。

步骤 5 点击其中一台设备的**查看对等体 (View Peers)**。

步骤 6 双击图表视图中报告问题的设备。

步骤 7 点击底部隧道详细信息面板中的**密钥交换 (Key Exchange)**。您将能够查看两台设备并从该点诊断关键问题。

查找为隧道定义的不完整或配置错误的访问列表

“不完整或配置错误的访问列表”条件只能出现在 ASA 设备上。

步骤 1 在 CDO 导航栏中，点击 **VPN** > **ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)** 以打开 VPN 页面。

步骤 2 选择**表视图 (Table View)**。

步骤 3 通过点击过滤器图标 打开过滤器面板。

步骤 4 选择每个报告问题的设备，然后查看右侧的“对等体”窗格。⚠对等体信息显示两个对等体。

步骤 5 点击其中一台设备的查看对等体。

步骤 6 双击图表视图中报告问题的设备。

步骤 7 点击底部隧道详细信息面板中的隧道详细信息。您将看到消息“网络策略：不完整”

查找隧道配置中的问题

在以下情况下可能会发生隧道配置错误：

- 当站点间 VPN 接口的 IP 地址更改时，“对等 IP 地址值已更改”。
- 当 VPN 隧道的 IKE 值与另一个 VPN 隧道不匹配时，系统将显示“IKE 值不匹配”消息。

步骤 1 在 CDO 导航栏中，点击 **VPN** > **ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)** 以打开 VPN 页面。

步骤 2 选择**表视图 (Table View)**。

步骤 3 通过点击过滤器图标 打开过滤器面板。

步骤 4 在**隧道问题 (Tunnel Issues)** 中，点击**检测到的问题 (Detected Issues)** 以查看 VPN 配置报告错误。您可以查看配置报告问题。⚠

步骤 5 选择 VPN 配置报告问题。

步骤 6 在右侧的“对等体”窗格中，会显示存在问题的对等体的图标。⚠将鼠标悬停在图标上可查看问题和解决方案。⚠

下一步：解决隧道配置问题。解决隧道配置问题, on page 78

解决隧道配置问题

此程序尝试解决以下隧道配置问题：

- 当站点间 VPN 接口的 IP 地址更改时，“对等 IP 地址值已更改”。

- 当 VPN 隧道的 IKE 值与另一个 VPN 隧道不匹配时，系统将显示“IKE 值不匹配”消息。

有关详细信息，请参阅查找隧道配置中的问题。

步骤 1 在 CDO 导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击相应的设备类型选项卡，然后选择与报告问题的 VPN 配置关联的设备。

步骤 4 接受设备更改。解决“检测到冲突”状态，第 173 页

步骤 5 在 CDO 导航窗格中，点击 **VPN** > **ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)** 以打开 VPN 页面。

步骤 6 选择报告此问题的 VPN 配置。

步骤 7 点击**操作 (Actions)** 窗格中的**编辑** 图标 。

步骤 8 在每个步骤中点击**下一步**，直到您在步骤 4 中点击**完成**按钮。

步骤 9 预览和部署所有设备的配置更改，第 160 页。

搜索和过滤器站点间 VPN 隧道

将过滤器边栏 与搜索字段结合使用，可重点搜索 VPN 隧道图中显示的 VPN 隧道。

步骤 1 在主导航栏中，导航至 **VPN > ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)**。

步骤 2 点击过滤器图标 可打开过滤器窗格。

步骤 3 使用以下过滤器细化搜索：

- **按设备过滤 (Filter by Device)** - 点击**按设备过滤 (Filter by Device)**，选择设备类型选项卡，然后选中要通过过滤查找的设备。
- **隧道问题 (Tunnel Issues)** - 我们是否检测到隧道的任一端存在问题。存在问题的设备的一些示例可能包括（但不限于）：缺少关联的接口或对等体 IP 地址或访问列表、IKEv1 提议不匹配等。（检测隧道问题尚不适用于 AWS VPC VPN 隧道。）
- **设备/服务 (Devices/Services)** - 按设备类型过滤。
- **状态 (Status)** - 隧道状态可以是活动或空闲。
  - **活动 (Active)** - 存在网络数据包通过 VPN 隧道的开放会话，或者已成功建立会话且尚未超时的会话。活动可以帮助指示隧道处于活动状态和相关性。
  - **空闲 (Idle)** - CDO 无法发现此隧道的开放会话，隧道可能未在使用或此隧道存在问题。
- **已载入 (Onboarded)** - 设备可以由 CDO 管理，也可以不由 CDO 管理（非托管）。
  - **托管 (Managed)** - 按 CDO 管理的设备过滤。
  - **非托管 (Unmanaged)** - 按 CDO 不管理的设备进行过滤。

- **设备类型 (Device Types)** - 隧道的任一端是实时（已连接设备）还是模型设备。

步骤 4 您还可以通过在搜索栏中输入设备名称或 IP 地址来搜索过滤结果。搜索不区分大小写。

载入非托管站点间 VPN 对等体

在载入其中一个对等设备时，CDO 将发现站点间 VPN 隧道。如果第二个对等设备不由 CDO 管理，则您可以过滤 VPN 隧道列表以查找非受管设备并将其载入：

步骤 1 在主导航栏中，选择 **VPN** > **ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)** 以打开 VPN 页面。

步骤 2 选择**表视图 (Table View)**。

步骤 3 通过点击 打开过滤器面板。

步骤 4 点击**非托管 (Unmanaged)**。

步骤 5 从表中的结果中选择一个隧道。

步骤 6 在右侧的**对等体 (Peers)** 窗格中，点击**载入设备 (Onboard Device)**，然后按照屏幕上的说明进行操作。

相关信息：

- 载入设备和服务
- 将 ASA 设备载入 CDO

查看站点间 VPN 隧道的 IKE 对象详细信息

您可以查看所选隧道的对等体/设备上配置的 IKE 对象的详细信息。这些详细信息根据 IKE 策略对象的优先级显示在层次结构中的树结构中。

Note 外联网设备不显示 IKE 对象详细信息。

步骤 1 在左侧 CDO 导航栏中，点击 **VPN > ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)**。

步骤 2 在 VPN Tunnels 页面中，点击连接对等体的 VPN 隧道的名称。

步骤 3 在右侧的“关系”下，展开要查看其详细信息的对象。

查看上次成功建立站点间 VPN 隧道的日期

步骤 1 查看 IPsec 站点间虚拟专用网络隧道信息。查看站点间 VPN 隧道信息, on page 81

步骤 2 点击 Tunnel Details 窗格。

步骤 3 查看上次查看的活动字段。

查看站点间 VPN 隧道信息

站点间 VPN 表视图是载入 CDO 的所有设备上可用的所有站点间 VPN 隧道的完整列表。隧道在此列表中仅存在一次。点击表中列出的隧道会在右侧栏中提供一个选项，以直接导航到隧道的对等体以进行进一步调查。

如果 CDO 不管理隧道的两端，您可以点击载入非托管站点间 VPN 对等体 以打开主载入页面并载入非托管对等设备。在 CDO 管理隧道两端的情况下，对等体 2 列包含受管设备的名称。但是，对于 AWS VPC，对等体 2 列包含 VPN 网关的 IP 地址。

要在表视图中查看站点间 VPN 连接，请执行以下操作：

步骤 1 在主导航栏中，点击 **VPN > ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)**。

步骤 2 点击**表格视图 (Table view)**  按钮。

步骤 3 使用搜索和过滤器站点间 VPN 隧道 以查找特定隧道，或放大全局视图图形以查找要查找的 VPN 网关及其对等体。

站点间 *VPN* 全局视图

步骤 1 在主导航栏中，点击 **VPN > ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)**。

步骤 2 点击**全局视图 (Global view)** 按钮。

步骤 3 使用搜索和过滤器站点间 VPN 隧道 以查找特定隧道，或放大全局视图图形以查找要查找的 VPN 网关及其对等体。

步骤 4 选择全局视图中表示的对等体之一。

步骤 5 点击**查看详细信息**。

步骤 6 点击 VPN 隧道的另一端，CDO 将显示该连接的隧道详细信息、NAT 信息和密钥交换信息：

- 隧道详细信息 - 显示有关隧道的名称和连接信息。点击刷新图标可更新隧道的连接信息。
- 特定于 AWS 连接的隧道详细信息 - AWS 站点到站点连接的隧道详细信息与其他连接略有不同。对于从 AWS VPC 到 VPN 网关的每个连接，AWS 会创建两个 VPN 隧道。这用于高可用性。
  - 隧道的名称代表您的 VPN 网关所连接的 VPC 的名称。隧道中指定的 IP 地址是您的 VPN 网关获知的 VPC 的 IP 地址。
  - 如果 CDO 连接状态显示为“活动”，则 AWS 隧道状态为“运行”。如果 CDO 连接状态为“非活动”，则 AWS 隧道状态为“关闭”。
- NAT 信息 - 显示正在使用的 NAT 规则类型、原始和转换后的数据包信息，并提供指向 NAT 表的链接以查看该隧道的 NAT 规则。（尚不可用于 AWS VPC 站点间 VPN。）

- 密钥交换 - 显示隧道和密钥交换问题正在使用的加密密钥。（尚不可用于 AWS VPC 站点间 VPN。）

站点间 *VPN* 隧道 *(Site-to-Site VPN Tunnels)* 窗格

Tunnels 窗格显示与特定 VPN 网关关联的所有隧道的列表。对于 VPN 网关和 AWS VPC 之间的站点间 VPN 连接，隧道窗格显示从 VPN 网关到 VPC 的所有隧道。由于您的 VPN 网关和 AWS VPC 之间的每个站点间 VPN 连接都有两个隧道，因此您会看到通常用于其他设备的隧道数量的两倍。

VPN 网关详细信息

显示连接到 VPN 网关的对等体的数量以及 VPN 网关的 IP 地址。这仅在“VPN 隧道”(VPN Tunnels) 页面中可见。

查看对等体

选择站点间VPN对等体后，对等体窗格将列出该对中的两台设备，并允许您点击其中一台设备的**查看对等体 (View Peer)**。通过点击**查看对等体 (View Peer)**，您可以看到与该设备关联的任何其他站点到站点对等体。这在“表”视图和“全局”视图中可见。

远程访问虚拟专用网络

远程访问虚拟专用网络 (RA VPN) 允许个人用户使用连接到互联网的计算机或其他受支持的 iOS 或 Android 设备，从远程位置连接到您的网络。这样，移动员工就可以从家庭网络或公共 Wi-Fi 网络进行连接。

RA VPN 配置包括以下组件：

- 连接配置文件：您可以创建远程访问 VPN 连接配置文件，允许用户在外部网络（例如其家庭网络）上时连接到您的内部网络。创建单独的配置文件，以适应不同的身份验证方法。连接配置文件由身份源和组策略组成。

相关信息：

- 为 ASA 配置远程访问虚拟专用网络, on page 82

为 ASA 配置远程访问虚拟专用网络

ASA 通过跨 TCP/IP 网络（如互联网）创建被用户视为专用连接的安全连接来创建远程访问虚拟专用网络 (VPN)。它可以创建单一用户到 LAN 连接和 LAN 到 LAN 连接。

这种安全连接被称为隧道，ASA 使用隧道协议来协商安全参数，创建并管理隧道，封装数据包，通过隧道收发数据包，然后再对它们解除封装。ASA 相当于一个双向隧道终端：可以接收普通数据包，封装它们，再将它们发送到隧道的另一端，在那里系统将对数据包解除封装并将其发送到最终目标。它也可以接收已封装的数据包，解除数据包封装，然后将它们发送到最终目标。

CDO 提供直观的用户界面，用于配置新的远程访问虚拟专用网络。它还允许您快速轻松地为 CDO 中载入的多个自适应安全设备 (ASA) 配置远程访问 VPN 连接。

CDO 允许您从头开始在 ASA 设备上配置远程访问 VPN 配置。它还允许您管理已使用其他 ASA 管理工具（例如自适应安全防御管理器 [ASDM] 或思科安全管理器 [CSM]）配置的远程访问 VPN 设置。当您载入已具有远程访问 VPN 设置的 ASA 设备时，CDO 会自动创建“默认远程访问 VPN 配置”并将ASA设备与此配置相关联。此默认配置可以包含设备上定义的所有连接配置文件对象。如果要了解读入 CDO 的 RAVPN 属性，请参阅管理和部署预先存在的 ASA 远程访问 VPN 配置部分。否则，您可以开始执行“ASA 的端到端远程访问 VPN 配置过程”部分中所述的步骤。

相关信息：

- ASA 的端到端远程访问 VPN 配置过程
  - 为 ASA 配置身份源
    - 创建 ASA Active Directory 领域对象
    - 创建 ASA RADIUS 服务器对象或组
  - 创建 ASA 远程访问 VPN 组策略, on page 89
  - 创建 ASA 远程访问 VPN 配置, on page 95
  - 配置 ASA 远程访问 VPN 连接配置文件, on page 99
- 管理和部署预先存在的 ASA 远程访问 VPN 配置
- 创建 IP 地址池
- 从 NAT 豁免远程访问流量, on page 112
- 验证 ASA 的远程访问 VPN 配置
- 查看 ASA 的远程访问 VPN 配置详细信息

ASA 的端到端远程访问 VPN 配置过程

本节提供在载入到 CDO 的 ASA 设备上配置远程访问 VPN 的端到端程序。

要为客户端启用远程访问 VPN，需要配置多个单独的项目。以下程序介绍了端到端流程。

步骤 1 配置用于对远程用户进行身份验证的身份源。有关详细信息，请参阅为 ASA 配置身份源。

您可以使用以下来源对尝试使用远程访问 VPN 连接到您的网络的用户进行身份验证。此外，可以使用客户端证书进行身份验证，可单独使用，也可与身份源配合使用。

- Active Directory 身份领域：作为主要身份验证源。在 Active Directory AD 服务器中定义用户账户。请参阅“配置 AD 身份领域”。请参阅创建 ASA Active Directory 领域对象。
- RADIUS 服务器组：充当主要或辅助身份验证源，并用于授权和记账。请参阅创建 ASA RADIUS 服务器对象或组。
- 本地身份源（本地用户数据库）：作为主要或回退源。您可以直接在设备上定义用户，不使用外部服务器。如果您使用本地数据库作为回退源，请确保您定义与外部服务器中描述的相同用户名/密码。注意：只能从自

适应安全设备管理器 (ASDM) 直接在 ASA 设备上创建用户帐户。请参阅《思科 ASA 系列防火墙 ASDM 配置指南，X.Y》的“访问控制对象”一章中的“配置本地用户组”部分。

步骤 2 （可选）创建 ASA 远程访问 VPN 组策略, on page 89。组策略定义用户相关的属性。可以配置组策略，根据组成员身份提供差异化的资源访问权限。或者，可以对所有连接使用默认策略。

步骤 3 创建 ASA 远程访问 VPN 配置, on page 95。

步骤 4 配置 ASA 远程访问 VPN 连接配置文件, on page 99。

步骤 5 （可选）从 NAT 豁免远程访问流量, on page 112。

步骤 6 将配置更改从 CDO 部署到 ASA。

Important 如果使用本地管理器（如自适应安全设备管理器 (ASDM)）更改远程访问 VPN 配置，CDO 中该设备的**配置状态 (Configuration Status)** 将显示“检测到冲突”(Conflict Detected)。请参阅 设备上的带外更改。您可以解决此 ASA 上的配置冲突。解决配置冲突, on page 172

What to do next

后续步骤

将远程访问 VPN 配置下载到 ASA 设备后，用户可以使用连接到互联网的计算机或其他受支持的 iOS 或 Android 设备从远程位置连接到您的网络。您可以从租户中所有已载入的 ASA 远程访问 VPN 前端监控实时 AnyConnect 远程访问 VPN 会话。请参阅监控远程访问虚拟专用网络会话。

为 *ASA* 配置身份源

身份源（例如 Microsoft Active Directory (AD) 领域和 RADIUS 服务器）是为组织内的人员定义用户账户的 AAA 服务器和数据库。身份源信息具有多种用途，例如提供与 IP 地址关联的用户身份，或是对远程访问 VPN 连接或到 CDO 的访问进行身份验证。

点击**对象 (Objects) > ASA 对象 (ASA Objects)**，然后点击 (+)> **身份源**以创建源。后期配置需要使用身份源的服务时，可以使用这些对象。您可以应用适当的过滤器来搜索现有源并对其进行管理。

确定目录基准标识名

配置目录属性时，需要为用户和组指定公共基准标识名 (DN)。基准在您的目录服务器中定义，并且会因网络而不同。您必须输入正确的基准，身份策略才能正常使用。如果基准错误，则系统无法确定用户名或组名，进而导致基于身份的策略无法使用。

Note 要获得正确的基准，请咨询目录服务器的管理员。

对于 Active Directory，您可以用域管理员的身份登录 Active Directory 服务器，并按照如下所示在命令提示符后输入 **dsquery** 命令来确定正确的基准：

用户搜索库

输入具有已知用户名（部分或完整）的 **dsquery user** 命令，以确定基准标识名。例如，以下命令使用部分名称“John*”返回以“John.”开头的所有用户的信息。

C:\Users\Administrator>dsquery user -name "John*"

"CN=John Doe,CN=Users,DC=csc-lab,DC=example,DC=com"

基准 DN 为“DC=csc-lab,DC=example,DC=com”。

组搜索基准

输入具有已知组名称的 **dsquery group** 命令，以确定基准标识名。例如，以下命令使用组名称 Employees 返回标识名：

C:\>dsquery group -name "Employees"

"CN=Employees,CN=Users,DC=csc-lab,DC=example,DC=com"

组基准 DN 为“DC=csc-lab,DC=example,DC=com”。

此外，您还可以使用 ADSI Edit 程序浏览 Active Directory 结构 (**Start** > **Run** > **adsiedit.msc**)。在 ADSI Edit 中，右键点击任意对象，例如组织单位 (OU)、组或用户，然后选择**属性 (Properties)** 查看标识名。然后，可以复制 DC 值的字符串作为基准。

要验证您是否获得了正确的基准，请执行以下操作：

步骤 1 点击目录属性中的“测试连接”(Test Connection) 按钮验证连接。解决所有问题后，保存目录属性。

步骤 2 提交对设备的更改。

步骤 3 创建访问规则，选择**用户**选项卡，并尝试从目录添加已知的用户和组名称。在您键入内容时，系统会自动填充建议，以匹配包含该目录的领域中的用户和组。如果这些建议显示在一个下拉列表中，则说明系统可以成功查询目录。如果您没有看到建议，而且确定您键入的字符串应显示在用户或组名称中，则需要更正相应的搜索基准。

What to do next

有关详细信息，请参阅创建 ASA Active Directory 领域对象。

RADIUS 服务器和组

您可以使用 RADIUS 服务器对管理用户进行身份验证和授权。配置要使用 RADIUS 服务器的功能时，您应选择 RADIUS 组而不是单个服务器。RADIUS 组所含 RADIUS 服务器是彼此副本的集合。如果一个组具有多个服务器，这些服务器可构成备份服务器链，在其中一台服务器不可用时提供冗余。但即使只有一台服务器，也必须创建包含一个成员的组，以配置功能的 RADIUS 支持。

您可以将此源用于以下目的：

- 远程访问 VPN 用作身份验证、授权和记账的身份源。您可以配合使用 AD 和 RADIUS 服务器。
- 身份策略，作为被动身份源来从远程访问 VPN 登录收集用户身份信息。

有关详细信息，请参阅创建 ASA RADIUS 服务器对象或组。

创建 ASA Active Directory 领域对象

当您创建或编辑身份源对象（例如 AD 领域对象）时，CDO 通过 SDC 将配置请求发送到 ASA 设备。然后，ASA 与配置的 AD 领域通信。

使用以下程序创建对象：

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > ASA 对象 (ASA Objects)**。

步骤 2 点击创建对象 () RA VPN 对象（ASA 和 FDM）身份源。 >

步骤 3 为对象输入**对象名称 (Object Name)**。

步骤 4 选择 **ASA** 作为**设备类型 (Device Type)**。

步骤 5 在向导的第一部分中，选择 Active Directory 领域作为身份源类型。点击**继续 (Continue)**。

步骤 6 配置基本领域属性。

- **目录用户名、目录密码 (Directory Username, Directory Password)** - 用户的标识名称和密码，该用户具备访问您要检索的用户信息的适当权限。对于 Active Directory，用户不需要更高的权限。您可以在域中指定任何用户。用户名必须是完全限定的；例如，Administrator@example.com（而不仅仅是 Administrator）。

  注释 系统使用此信息生成 ldap-login-dn 和 ldap-login-password。例如，Administrator@example.com 被转换为 cn=administrator,cn=users,dc=example,dc=com。请注意，cn = users 始终是此转换的一部分，因此您必须在公用名“users”文件夹下配置此处指定的用户。

- **基准区别名称 (Base Distinguished Name)** - 用于搜索或查询用户和组信息的目录树，即用户和组的公共父项。例如，cn=users,dc=example,dc=com。

步骤 7 配置目录服务器属性。

- **主机名/IP 地址** - 目录服务器的主机名或 IP 地址。如果以加密方式连接到服务器，则必须输入完全限定域名，而非 IP 地址。
- **端口** - 用于与服务器通信的端口号。默认值为 389。如果选择 LDAPS 作为加密方法，请使用端口 636。
- Encryption - 要使用加密连接下载用户和组信息，请选择 LDAPS 以使用 SSL 保护 ASA 与 LDAP 服务器之间的通信。它需要基于 SSL 的 LDAP。使用端口 636。

  系统默认为**无**，也就是说以明文形式下载用户和组信息。

步骤 8 （可选）使用测试按钮验证配置。

步骤 9 （可选）点击添加其他配置，将多个 Active Directory (AD) 服务器添加到 AD 领域。AD 服务器需要彼此复制并支持相同的 AD 域。因此，与该 AD 领域关联的所有 AD 服务器的基本领域属性（例如目录名称、目录密码和基本可分辨名称）必须相同。

步骤 10 点击 **Add**。

编辑 ASA Active Directory 领域对象

请注意，在编辑身份源对象时，不能更改身份源类型。您必须创建具有正确类型的新对象。

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > ASA 对象 (ASA Objects)**。

步骤 2 使用对象过滤器和搜索字段找到要编辑的对象。

步骤 3 选择要编辑的对象。

步骤 4 点击**操作 (Actions)** 窗格中的编辑图标 。

步骤 5 以在上述过程中创建值的相同方式编辑对话框中的值。展开下面列出的配置栏，以编辑或测试主机名/IP 地址或加密信息。

步骤 6 点击**保存 (Save)**。

步骤 7 CDO 显示将受更改影响的策略。点击**确认 (Confirm)** 以完成对对象和受其影响的任何策略的更改。

步骤 8 立即将配置更改从 CDO 部署到 ASA您所做的更改，或等待并一次部署多个更改。

创建 ASA RADIUS 服务器对象或组

在创建或编辑 RADIUS 服务器对象或一组 RADIUS 服务器对象等身份源对象时，CDO 会通过 SDC 将配置请求发送到 ASA 设备。

创建 ASA RADIUS 服务器对象

RADIUS 服务器提供 AAA（身份验证、授权和记账）服务。

使用以下程序创建对象：

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > ASA 对象 (ASA Objects)**。

步骤 2 点击**创建对象 (Create Object)** ( )**> RA VPN 对象 (ASA & FDM) (RA VPN Objects [ASA & FDM])** > **身份源 (Identity Source)**。

步骤 3 为对象输入**对象名称 (Object name)**。

步骤 4 选择 **ASA** 作为**设备类型 (Device Type)**。

步骤 5 选择 RADIUS 服务器作为身份源类型。点击**继续 (Continue)**。

步骤 6 使用以下属性编辑身份源配置：

- **服务器名称或 IP 地址 (Server Name or IP Address)** - 服务器的完全限定主机名 (FQDN) 或 IP 地址。
- **身份验证端口 (Authentication Port)**（可选）- 在其上执行 RADIUS 身份验证和授权的端口。默认值为 1812。
- **超时 (Timeout)** - 系统将请求发送至下一服务器之前等待服务器响应的时长，此为 1-300 秒之间的数值。默认值为 10 秒。
- 输入**服务器密钥 (Server Secret Key)**（可选）- 用于加密 ASA 设备和 RADIUS 服务器之间数据的共享密钥。该密钥是一个区分大小写的字母数字字符串，最多 64 个字符，且不含空格。密钥必须以字母数字字符或下划线开头，它可以包含特殊字符：$ & - _ . + @。字符串必须匹配 RADIUS 服务器上配置的字符串。如果不配置密钥，则不加密连接。

步骤 7 点击**添加 (Add)**。

步骤 8 立即将配置更改从 CDO 部署到 ASA您所做的更改，或等待并一次部署多个更改。

创建 ASA RADIUS 服务器组

RADIUS 服务器组中包含一个或多个 RADIUS 服务器对象。组中的服务器必须是彼此的备份。这些服务器构成备份服务器链，因此，如果第一台服务器不可用，系统可以尝试列表中的下一个服务器。

使用以下程序创建对象组：

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > ASA 对象 (ASA Objects)**。

步骤 2 点击创建对象 () RA VPN 对象（ASA 和 FDM）身份源。 

步骤 3 为对象输入**对象名称 (Object name)**。

步骤 4 选择 **ASA** 作为**设备类型 (Device Type)**。

步骤 5 选择 RADIUS 服务器组作为身份源类型。 点击**继续 (Continue)**。

步骤 6 使用以下属性编辑身份源配置：

- **断路时间 (Dead Time)** - 只有当所有服务器均发生故障时，才会重新激活故障服务器。断路时间是指最后一台服务器发生故障后，在重新激活所有服务器之前所等待的时间。
- **最大失败尝试次数 (Maximum Failed Attempts)** - 尝试组中下一个服务器之前发送到 RADIUS 服务器的失败请求（即，未收到响应的请求）数。超过最大失败尝试次数时，系统会将服务器标记为故障。对于给定功能，如果您使用本地数据库配置回退方法，并且组中的所有服务器都无法响应，则会将该组视为无法响应，并将尝试回退方法。该服务器组会在断路时间内保持标记为无响应，以确保该时段内其他 AAA 请求不会尝试联系该服务器组，而是立即使用回退方法。
- **动态授权/端口 (Dynamic Authorization/Port)**（可选）- 如果为此 RADIUS 服务器组启用 RADIUS 动态授权或授权更改 (CoA) 服务，该组会注册 CoA 通知并侦听指定的端口，以便使 CoA 策略从 Cisco Identity Services Engine (ISE) 进行更新。仅当您在远程访问 VPN 中结合 ISE 使用此服务器组时，才能启用动态授权。

步骤 7 从下拉菜单中选择支持 RADIUS 服务器的 AD 领域。如果尚未创建 AD 领域，请从下拉菜单中点击创建。

步骤 8 点击 RADIUS 服务器添加按钮，添加现有的 RADIUS 服务器对象。  或者，您可以从此窗口创建新的 RADIUS 服务器对象。

Note 优先级添加这些对象，因为列表中的第一个服务器将被使用，直到它停止响应。然后，ASA 默认使用列表中的下一个服务器。

步骤 9 立即将配置更改从 CDO 部署到 ASA您所做的更改，或等待并一次部署多个更改。

编辑 ASA Radius 服务器对象或组

使用以下程序编辑 Radius 服务器对象或 Radius 服务器组：

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > ASA 对象 (ASA Objects)**。

步骤 2 使用对象过滤器和搜索字段找到要编辑的对象。

步骤 3 选择要编辑的对象。

步骤 4 点击**操作 (Actions)** 窗格中的编辑图标 。

步骤 5 以在上述过程中创建值的相同方式编辑对话框中的值。要编辑或测试主机名/IP 地址或加密信息，请展开配置栏。

步骤 6 点击**保存 (Save)**。

步骤 7 CDO 显示将受更改影响的策略。点击**确认 (Confirm)** 以完成对对象和受其影响的任何策略的更改。

步骤 8 立即将配置更改从 CDO 部署到 ASA您所做的更改，或等待并一次部署多个更改。

创建 *ASA* 远程访问 *VPN* 组策略

组策略是一组面向用户的远程访问 VPN 的属性/值对。连接配置文件使用组策略在建立隧道后设置用户连接的条款。通过组策略可将整组属性应用于用户或用户组，而不必为每个用户单独指定每个属性。

系统包含名为“DfltGrpPolicy”的默认组策略。您可以创建其他组策略，以提供您所需的服务。

注释 不能将不一致的组策略对象添加到远程访问 VPN 配置。在将组策略添加到远程访问 VPN 配置之前，请解决所有不一致问题。

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > ASA 对象 (ASA Objects)**。

步骤 2 点击“加号” 按钮。

步骤 3 点击 **RA VPN 对象（ASA 和 FDM）(RA VPN Objects [ASA & FDM]) > RA VPN 组策略 (RA VPN Group Policy)**。

步骤 4 输入组策略的名称。此名称最多可包含 64 个字符，允许使用空格。

步骤 5 在**设备类型 (Device Type)** 下拉列表中，选择 **ASA**。

步骤 6 执行以下任一操作：

- 点击所需的选项卡并配置页面上的属性：
  - ASA 远程访问 VPN 组策略属性
  - AnyConnect 客户端配置文件， 第 90 页
  - 会话设置属性， 第 91 页
  - 地址分配属性， 第 91 页
  - 分割隧道属性， 第 92 页
  - AnyConnect 属性， 第 93 页

- 流量过滤器属性，第 94 页
- Windows 浏览器代理属性，第 95 页

步骤 7 点击**保存 (Save)** 以保存组策略。

ASA 远程访问 VPN 组策略属性

本节介绍与 ASA 远程访问 VPN 组策略关联的属性。

常规属性

组策略的常规属性定义组名称和一些其他基本设置。

- **DNS 服务器**：输入连接到 VPN 时用于域名解析的 DNS 服务器的 IP 地址。可以使用逗号分隔地址。
- **横幅**：登录时向用户显示的横幅文本或欢迎消息。默认无横幅。最多 496 字符。AnyConnect 客户端支持部分 HTML。为确保向远程用户正确地显示横幅，请使用
 标记表示换行。
- **默认域 (Default Domain)**：远程访问 VPN 中用户的默认域名。例如 example.com。此域将被添加到非完全限定的主机名，例如 serverA 而不是 serverA.example.com。

AnyConnect 客户端配置文件

运行软件版本 6.7 或更高版本的 FTD 支持此功能。

Cisco AnyConnect VPN 客户端通过各种内置模块提供增强的安全性。这些模块提供网络安全，终端流量的网络可视性和网络外漫游保护等服务。每个客户端模块都包含一个客户端配置文件，其中包含根据您的要求的一组自定义配置。

当 VPN 用户下载 VPN AnyConnect 客户端软件时，您可以选择要下载到客户端的 AnyConnect VPN 配置文件对象和 AnyConnect 模块。

1. 选择或创建 AnyConnect VPN 配置文件对象。请参阅上传 RA AnyConnect 客户端配置文件, on page 115。除 DART 和“登录前启动”模块外，必须选择 AnyConnect VPN 配置文件对象。
2. 点击**添加Any 链接客户端模块 (Add Any Connect Client Module)**。

   以下 AnyConnect 模块是可选的，您可以将这些模块配置为在 VPN AnyConnect 客户端软件时下载：

   - **AMP 启用程序 (AMP Enabler)** - 为终端部署高级恶意软件防护 (AMP) 。
   - **DART** - 捕获系统日志和其他诊断信息的快照并在桌面上创建 .zip 文件，因此您可以便利地将故障排除信息发送到思科 TAC。
   - **反馈 (Feedback)** - 提供有关客户已启用和使用的功能和模块的信息。
   - **ISE 终端安全评估 (ISE Posture)** - 使用 OPSWAT v3 库执行终端安全评估检查，评估终端的合规性。

- **网络访问管理器 (Network Access Manager)** - 为有线和无线网络访问提供 802.1X（第 2 层）和设备身份验证。
- **网络可视性 (Network Visibility)** - 可提升企业管理员执行容量和服务规划、审计、合规性和安全分析的能力。
- **登录前启动 (Start Before Login)** - 通过在 Windows 登录对话框出现之前启动 AnyConnect，强制用户在登录到 Windows 之前通过 VPN 连接而连接到企业基础设施。
- **Umbrella 漫游安全 (Umbrella Roaming Security)** - 在没有处于活动状态的 VPN 时提供 DNS 层安全。
- **网络安全 (Web Security)** - 根据定义的安全策略分析网页的元素，允许可接受的内容，并阻止恶意或不可接受的内容。

3. 在**客户端模块 (Client Module)** 列表中选择 **AnyConnect 模块 (AnyConnect module)**。
4. 在**配置文件 (Profile)** 列表中，选择或创建包含 AnyConnect 客户端配置文件的配置文件对象。
5. 选择**启用模块下载 (Enable Module Download)** 以下载客户端模块以及配置文件。如果未选择，则终端只能下载客户端配置文件。

会话设置属性

组政策会话设置控制用户可以连接到 VPN 的时长和可以创建的独立连接的数量。

- **最长连接时间 (Maximum Connection Time)**：在不注销和重新连接的情况下，用户可持续连接到 VPN 的最大时间长度（以分钟为单位），范围为 1 到 4473924 或留空。默认值为无限（留空），但空闲超时仍适用。
- **连接时间警报间隔 (Connection Time Alert Interval)**：如果您指定了最大连接时间，则警报间隔定义，在达到最长时间之前，向用户显示即将自动断开连接警告的时间。用户可以选择结束连接并重新连接，以重新启动计时器。默认值为 1 分钟。可以指定 1 到 30 分钟。
- **空闲时间 (Idle Time)**：VPN 连接在自动关闭之前可以闲置的时间长度（以分钟为单位），范围为 1 到 35791394。如果在此时间段内此连接上无通信活动，则系统会终止连接。默认值为 30 分钟。
- **空闲时间警报间隔 (Idle Time Alert Interval)**：在达到空闲时间之前，向用户显示因闲置会话而即将自动断开连接的警报的时间。任何活动都会重置计时器。默认值为 1 分钟。可以指定 1 到 30 分钟。
- **每个用户的同时登录数 (Simultaneous Login Per User)**：允许用户执行的最多同时登录数。默认值为 3。可以指定 1 到 2147483647 个连接。允许许多同时连接可能会危害安全性并影响性能。

地址分配属性

组策略的地址分配属性定义组的 IP 地址池。此处定义的地址池将覆盖使用此组的任何连接配置文件中定义的池。如果您希望使用连接配置文件中定义的池，请将这些设置留空。

- **IPv4 地址池 (IPv4 Address Pool)、IPv6 地址池 (IPv6 Address Pool)**：这些选项定义远程终端的地址池。根据客户端用于建立 VPN 连接的 IP 版本，从这些池为客户端分配地址。选择 IP 地址池，定义要支持的每个 IP 类型的子网。如果您不想支持该 IP 版本，则可以空着列表。例如，可以将 IPv4 池定义为 10.100.10.0/24。地址池不能与外部接口的 IP 地址位于同一子网。创建新的创建IP地址池。可以指定包含最多六个地址池的列表，用于本地地址分配。地址池的指定顺序非常重要。系统按照地址池出现的顺序分配这些地址池中的地址。**注意**：可为同一个组策略同时配置 IPv4 和 IPv6 地址池。如果在同一个组策略中配置了两个版本的 IP 地址，则配置了 IPv4 的客户端将获得 IPv4 地址，配置了 IPv6 的客户端将获得 IPv6 地址，而同时配置了 IPv4 和 IPv6 地址的客户端将获得 IPv4 和 IPv6 地址。
- **DHCP 范围 (DHCP Scope)**：如果在连接配置文件中为地址池配置了 DHCP 服务器，DHCP 作用域会标识要用于此组的地址池的子网。DHCP 服务器的地址还必须来自此作用域标识的同一个池。作用域允许您选择DHCP服务器中定义的部分地址池，用于此特定组。如未定义网络范围，则 DHCP 服务器将按地址池配置顺序分配 IP 地址。它将检查各个池，直到发现未分配的地址为止。要指定作用域，请输入包含网络号主机地址的网络对象。例如，要告诉 DHCP 服务器使用 192.168.5.0/24 子网池中的地址，请输入指定 192.168.5.0 为主机地址的网络对象。DHCP 仅可用于 IPv4 寻址。

分割隧道属性

组策略的分割隧道属性定义系统如何处理用于内部网络的流量和流向外部的流量。分割隧道引导一些网络流量通过 VPN 隧道（加密），将剩下的网络流量引导至 VPN 隧道外部（未加密或以明文形式）。

典型地，在远程访问 VPN 中，您可能希望 VPN 用户通过您的设备访问互联网。但是，您可以允许 VPN 用户在连接到远程访问 VPN 时访问外部网络。这种技术有时候称为分割隧道或发夹方法。拆分隧道不仅允许 VPN 通过安全隧道连接到远程网络，而且允许连接到 VPN 隧道外的网络。拆分隧道可减少 FTD 设备上的网络负载，并增加外部接口上的带宽。

准备工作

为 IPv4 网络创建一个分割隧道策略并为 IPv6 网络创建另一个分割隧道策略，则指定的访问列表同时用于两种协议。因此，访问列表应同时包含 IPv4 和 IPv6 流量的访问控制项 (ACE)。

当 ASA 设备载入 CDO 时，它会读取与该设备关联的扩展 ACL。有关详细信息，请参阅组策略 。如果要创建新的 ACL，请参阅 ASA 策略（扩展访问列表）以进行创建。

Note 确保在要创建的 ACL 中将用于分割隧道的网络指定为源网络。

- **IPv4 分割隧道 (IPv4 Split Tunneling)、IPv6 分割隧道 (IPv6 Split Tunneling)**：可以根据流量是使用 IPv4 寻址还是 IPv6 寻址来指定不同的选项，但每个流量的选项都相同。如果想要启用分割隧道，指定其中一个要求您选择网络对象的选项。
  - **允许所有流量通过隧道 (Allow all traffic over tunnel)**：不分割隧道。一旦用户建立远程访问VPN连接，用户的所有流量都会通过受保护隧道。这是默认值。这也被视为最安全的选项。

- **允许指定的流量通过隧道**：选择定义源网络的扩展访问列表。任何来自这些源的流量都会通过受保护隧道。客户端会将前往其他目标的流量路由至隧道外部（例如，本地 Wi-Fi 或网络连接）。
- **排除以下指定网络**：选择定义源网络的网络对象。客户端将来自这些源的任何流量路由到隧道外部的连接。来自任何其他来源的流量通过隧道。
- **网络列表**：选择可以同时具有 IPv4 和 IPv6 网络的扩展 ACL 网络。

- **分割 DNS**：您可以配置系统通过安全连接发送某些 DNS 请求，同时允许客户端将其他 DNS 请求发送到客户端上配置的 DNS 服务器。您可以配置以下 DNS 行为：
  - **根据分割隧道策略发送 DNS 请求 (Send DNS Request as per split tunnel policy)**：使用此选项时，系统将按照与定义分割隧道选项相同的方式处理DNS请求。如果启用分割隧道，则会根据目标地址发送 DNS 请求。如果未启用分割隧道，所有 DNS 请求都会通过受保护的连接。
  - **始终通过隧道发送 DNS 请求 (Always send DNS requests over tunnel)**：如果启用了分割隧道，但想要通过受保护连接将所有 DNS 请求发送到为该组定义的 DNS 服务器上，则可选择此选项。
  - **仅通过隧道发送指定的域 (Send only specified domains over tunnel)**：如果想要让受保护的 DNS 服务器仅解析特定域的地址，则可选择此选项。然后，指定这些域，用逗号分隔域名。例如，example.com, example1.com。如果想要让内部 DNS 服务器解析内部域的名称，同时让外部 DNS 服务器处理所有其他互联网流量，请使用此选项。

AnyConnect 属性

组策略的 AnyConnect 属性定义 AnyConnect 客户端用于远程访问 VPN 连接的某些 SSL 和连接设置。

- **SSL 设置**
  - **启用数据报传输层安全 (DTLS) (Enable Datagram Transport Layer Security [DTLS])**：是否允许 AnyConnect 客户端使用两个同步隧道：SSL 隧道和 DTLS 隧道。使用 DTLS 可避免某些 SSL 连接带来的延迟和带宽问题，并可改进对数据包延迟敏感的实时应用的性能。如果不启用 DTLS，AnyConnect 客户端用户在建立 SSL VPN 连接时仅与 SSL 隧道连接。
  - **DTLS 压缩 (DTLS Compression)**：是否使用 LZS 为此组压缩数据报传输层安全 (DTLS) 连接。默认情况下会禁用 DTLS 压缩。
  - **SSL 压缩 (SSL Compression)**：是否启用数据压缩，如启用，则设置要使用的数据压缩方法：**Deflate** 或 **LZS**。默认情况下会**禁用** SSL 压缩。数据压缩加快了传输速率，但也增加了每个用户会话的内存需求和 CPU 使用率。因此，SSL 压缩会降低设备的整体吞吐量。
  - **SSL 重新生成密钥方法 (SSL Rekey Method)**、**SSL 重新生成密钥间隔 (SSL Rekey Interval)**：客户端能够为VPN连接重新生成密钥，重新协商加密密钥和初始化向量，从而提高连接的安全性。选择**无**可禁用重新生成密钥。要启用重新生成密钥，请选择 **新隧道 (New Tunnel)** 来创建新的隧道。（ **现有隧道 (Existing Tunnel)** 选项导致的操作与 **新隧道 (New Tunnel)** 的相同。）如果启用重新生成密钥，还需设置重新生成密钥间隔，默认间隔为 4 分钟。可以将间隔设置为 4 到 10080 分钟（1 周）。

- 连接设置
  - **忽略 DF（不分片）位 (Ignore the DF [Don't Fragment] bit)**：是否忽略需要分片的数据包内的“不分片” (DF) 位。选择此选项会允许强制将已设置 DF 位的数据包分片，从而使这些数据包能够通过隧道。
  - **客户端绕行协议**：允许您配置安全网关管理 IPv4 流量（安全网关仅允许 IPv6 流量时）或管理 IPv6 流量（安全网关仅允许 IPv4 流量时）的方式。

    当 AnyConnect 客户端建立与头端的 VPN 连接时，头端可以为客户端分配 IPv4 和/或 IPv6 地址。如果头端对 AnyConnect 连接仅分配一个 IPv4 地址或一个 IPv6 地址，则您可以配置 Client Bypass Protocol 以丢弃头端尚未分配 IP 地址（默认、已禁用、未检查）的网络流量，或允许该流量绕过头端并从客户端以未加密或“明文形式”发送（已启用、已检查）。

    例如，假设安全网关只将一个 IPv4 地址分配给 AnyConnect 连接，且终端为双协议栈。当终端尝试访问 IPv6 地址时，如果禁用客户端旁路协议，则会丢弃 IPv6 流量；但是，如果启用客户端旁路协议，则会从客户端以明文形式发送 IPv6 流量。
  - **MTU**：思科 AnyConnect VPN 客户端为 SSL VPN 连接建立的最大传输单位 (MTU) 大小。默认值为 1406 字节。范围为 576 至 1462 字节。
    - **AnyConnect 和 VPN 网关之间的保持连接消息**：是否在对等体之间交换保持连接消息，以证明它们可用于在隧道中发送和接收数据。保持连接消息以设置的时间间隔传输。默认间隔为 20 秒，有效范围为 15 到 600 秒。
    - **网关端 DPD 间隔、客户端 DPD 间隔**：启用失效对等体检测 (DPD)，确保 VPN 网关或 VPN 客户端快速检测对等体不再响应的时间。您可以单独启用网关或客户端 DPD。发送 DPD 消息的默认间隔为 30 秒。时间间隔可以是 5 到 3600 秒。

流量过滤器属性

组策略的流量过滤器属性定义您想要对分配到该组的用户设置的限制。您可以使用这些属性（而非创建策略规则）根据主机或子网地址和协议或 VLAN 来限制远程访问 VPN 用户仅可访问特定资源。默认情况下，远程访问 VPN 用户不会受到组策略的限制，可以访问受保护网络上的任何目标。

- **访问列表过滤器 (Access List Filter)**：使用扩展的访问控制列表 (ACL) 限制访问权限。选择 Smart CLI 扩展 ACL 对象。扩展 ACL 允许您基于源地址、目的地址和协议（例如 IP 或 TCP）进行过滤。ACL 评估遵循自上而下、“先匹配的规则先应用”原则，因此，请确保特定规则放在一般规则之前。ACL 末尾不包含隐式“deny any”语句，因此如果您想要拒绝对几个子网的访问，同时允许其他访问，请确保在 ACL 末尾加上“permit any”规则。由于您无法在编辑扩展的 ACL Smart CLI 对象时创建网络对象，因此您应在编辑组策略之前创建 ACL。否则，您可能需要先创建对象，然后再返回来创建网络对象，最后创建您需要的所有访问控制条目。要创建 ACL，登录 FDM，请转至**设备 (Device)** > **高级配置 (Advanced Configuration)** > **智能 CLI (Smart CLI)** > **对象 (Objects)**，创建对象，并选择**扩展访问列表 (Extended Access List)** 作为对象类型。
- **限制 VPN 到 VLAN (Restrict VPN to VLAN)**：也称为“VLAN 映射”，此属性指定该组策略应用到的会话的出口 VLAN 接口。系统将该组中的所有流量都转发到所选 VLAN。使用此属性向组策略分配 VLAN 以简化访问控制。向此属性赋值是在会话中使用 ACL 过滤流量的替代方法。确保您指定了在设备子接口上定义的 VLAN 编号。值的范围为 1 到 4094。

Windows 浏览器代理属性

组策略的 Windows 浏览器代理属性确定用户浏览器上定义的代理是否运行以及如何运行。

可以为 **VPN 会话期间浏览器代理**选择以下值之一：

- **终端设置无变化 (No change in endpoint settings)**：允许用户配置（或不配置）浏览器代理或 HTTP，并在已配置的情况下使用代理。
- **禁用浏览器代理 (Disable browser proxy)**：不使用为浏览器定义的代理（如有）。浏览器连接不会通过该代理。
- **自动检测设置 (Auto detect settings)**：在客户端设备的浏览器中启用自动代理服务器检测。
- **使用自定义设置 (Use custom settings)**：定义所有客户端设备应对 HTTP 流量使用的代理。配置以下设置：
  - **代理服务器 IP 或主机名 (Proxy Server IP or Hostname)、端口 (Port)**：代理服务器的 IP 地址或主机名，以及代理服务器用于代理连接的端口。主机和端口总共不能超过 100 个字符。
  - **浏览器例外列表 (Browser Proxy Exemption List)**：与例外列表中的主机/端口的连接不通过代理。添加不应使用代理的所有目标的主机/端口值。例如，www.example.com 端口 80。点击**添加代理例外 (Add proxy exemption)** 以将项目添加到列表。点击垃圾桶图标可删除项目。整个代理例外列表（包括所有地址和端口）不能超过 255 个字符。

创建 *ASA* 远程访问 *VPN* 配置

CDO 允许您将一个或多个自适应安全设备 (ASA) 设备添加到远程访问 VPN 配置向导，并配置与设备关联的 VPN 接口、访问控制和 NAT 豁免设置。因此，每个远程访问 VPN 配置都可以在与远程访问 VPN 配置关联的多个 ASA 设备之间共享连接配置文件和组策略。此外，您可以通过创建连接配置文件和组策略来增强配置。

您可以载入已配置远程访问 VPN 设置的 ASA 设备，也可以载入没有远程访问 VPN 设置的新设备。请参阅将 ASA 设备载入 CDO。当您载入已具有远程访问 VPN 设置的 ASA 设备时，CDO 会自动创建“默认远程访问 VPN 配置”并将 ASA 设备与此配置相关联。此外，此默认配置可以包含设备上定义的所有连接配置文件对象。有关详细信息，请参阅管理和部署预先存在的 ASA 远程访问 VPN 配置。CDO 允许您删除默认配置。

重要事项

- 不允许在同一远程访问 VPN 配置中添加 ASA 和 FTD。
- 一台 ASA 设备不能有多个远程访问 VPN 配置。

开始之前

在将 ASA 设备添加到远程访问 VPN 配置之前，ASA 设备必须满足以下前提条件：

- 许可证要求。

  必须启用设备才能使用出口控制功能。

要查看 ASA 设备的许可证摘要，请在 ASA 命令行界面中执行 show license summary 命令。要使用 CDO ASA CLI 界面，请参阅在 CDO 界面中使用 ASA CLI。

- 许可证摘要中启用的出口控制功能示例：

注册：状态：已注册智能账户：Cisco SVS temp-request access license@cisco.com 出口控制功能：ALLOWED http://licensing@cisco.com

```
Last Renewal Attempt: None

Next Renewal Attempt: Jun 08 2021 09:46:22 UTC
```

要创建或编辑 VPN 配置，“导出控制功能”属性必须处于“允许”状态。

如果该属性处于“不允许”(Not Allowed) 状态，CDO 将在创建或修改 VPN 配置时显示错误信息（“无法为不符合出口标准的设备配置远程访问 VPN。”[remote access VPN cannot be configured for devices which are not export compliant.]），并且不允许在设备上配置远程访问 VPN。

- 设备身份证书。

  对客户端与 ASA 设备之间的连接进行身份验证需要使用证书。在开始 VPN 配置之前，请确保身份证书已存在于 ASA 设备上。

  要确定设备上是否存在证书，请在 ASA 命令行界面中执行 show crypto CA Certificates 命令。要使用 CDO ASA CLI 界面，请参阅在 CDO 界面中使用 ASA CLI。

  如果身份证书不存在或者您想要注册新证书，请使用 CDO 在 ASA 上安装它们。请参阅 ASA 证书管理。

  中介绍了数字证书在远程访问 VPN 环境中的使用。远程访问 VPN 基于证书的身份验证，第 111 页

- 外部接口。

  必须已在 ASA 设备上配置外部接口。您需要使用 ASDM 或 ASA CLI 来配置接口。 要了解如何使用 ASDM 配置接口，请参阅《思科 ASA 系列常规操作 CLI 配置指南 X.Y》的“接口”一书。

- 下载 AnyConnect 软件包并将其上传到远程服务器。稍后，使用远程访问 VPN 向导或 ASA 文件管理向导将 AnyConnect 软件包从服务器上传到 ASA。有关说明，请参阅管理 ASA 设备上的 AnyConnect 软件包。

- 没有待处理的配置部署。

- 如果使用本地数据库进行身份验证，请使用 ASDM 或 ASA CLI 将用户账户添加到本地数据库。

  要使用 ASDM 添加用户帐户，请参阅《思科 ASA 系列 VPN CLI 配置指南，X.Y》的“AAA 服务器和本地数据库”一书中的“将用户帐户添加到本地数据库”部分。

  要使用 ASA CLI 添加用户账户，请执行 username password priv_level] 命令。**username[] password [] privilege [**

- ASA 更改会同步到 CDO。

  1. 在左侧的 CDO 导航栏中，点击**清单 (Inventory)** 并搜索一个或多个要同步的 ASA 设备。
  2. 选择一个或多个设备，然后点击检查更改。CDO 与一个或多个 FTD 设备通信以同步更改。

- 远程访问 VPN 配置组策略对象一致。
  - 确保解决所有不一致的组策略对象，因为它们无法添加到远程访问VPN配置中。解决问题或从“对象”(Objects) 页面删除不一致的组策略对象。有关详细信息，请参阅解决重复对象问题和解决不一致对象问题。

步骤 1 将 ASA 设备载入 CDO。

步骤 2 在左侧的 CDO 导航栏中，点击 VPN ASA/FDM 远程访问 VPN 配置。 >

步骤 3 点击蓝色加号  按钮以创建远程访问 VPN 配置。

步骤 4 输入远程访问 VPN 配置的名称。

步骤 5 点击蓝色加号 () 按钮将 ASA 设备添加到配置。

您可以添加设备详细信息并配置与设备关联的网络流量相关权限。

1. 提供以下设备详细信息：
   - 设备：选择要添加的ASA设备，然后点击选择。重要提示：不允许在同一远程访问VPN配置中添加ASA和FTD。
   - **设备身份证书 (Certificate of Device Identity)**：选择用于建立设备身份的内部证书。在 AnyConnect 客户端与设备进行连接时确定客户端的设备身份。客户端必须接受此证书才能完成安全的 VPN 连接。
   - **外部接口 (Outside Interface)**：选择用户在进行远程访问 VPN 连接时连接的接口。请选择您使用此连接配置文件支持的设备与最终用户之间的任何接口，虽然这通常是外部（面向互联网的）接口。

     注意 您无法为不符合导出要求的设备创建或修改远程访问 VPN 配置。您必须在启用出口控制功能的情况下许可 ASA 设备，然后重试。

2. 点击继续以配置流量权限。
   - **为已解密的流量绕过访问控制策略 (sysopt permit-vpn)**：默认情况下，已解密流量要经过访问控制策略的检查。启用此选项可绕过解密流量选项，绕过访问控制策略检查，但从AAA服务器下载的VPN筛选ACL和授权 ACL 仍会应用于 VPN 流量。

     请注意，如果选择此选项，系统会配置 sysopt connection permit-vpn 命令，此为全局设置。这也会影响站点间 VPN 连接的行为。

     如果不选择此选项，外部用户可能会骗取远程访问 VPN 地址池中的 IP 地址，从而获取访问您网络的权限。这种情况可能会发生，因为您创建的访问控制规则需要允许地址池访问内部资源。如果您使用访问控制规则，请考虑使用用户说明来控制访问，而不是只使用源 IP 地址。

     选择此选项的弊端在于，VPN 流量将不会被检测，也就是说不会对流量应用入侵和文件保护、URL 过滤或其他高级功能。同时，系统不会生成有关此流量的任何连接事件，且统计控制面板不会反映VPN连接。
   - **NAT 豁免 (NAT Exempt)**：NAT 豁免将豁免转换地址，并允许已转换的主机和远程主机发起与受保护主机的连接。配置 NAT 免除，使进出远程访问 VPN 终端的流量免于执行 NAT 转换。请参阅从 NAT 豁免远程访问流量，第 112 页。

3. 点击**确定 (OK)**。

“检测到的 AnyConnect 软件包”显示设备上已有的 AnyConnect 软件包。

有两个选项可用于从远程访问 VPN 向导将 AnyConnect 软件包上传到 ASA：

- （选项 1）：从 CDO 的存储库中选择一个软件包。ASA 必须能够访问互联网。
- （选项 2）：指定预加载 AnyConnect 软件包的 ftp/http/https/scp/smb/tftp URL 位置。

有关说明，请参阅管理 ASA 设备上的 AnyConnect 软件包。

注释 注意：如果要替换现有软件包，请参阅管理 ASA 设备上的 AnyConnect 软件包。

步骤 6 点击**确定 (OK)**。

ASA VPN 配置已创建。

修改 ASA 远程访问 VPN 配置

您可以修改现有远程访问 VPN 配置的名称和设备详细信息。

步骤 1 选择要修改的配置，然后在操作下点击编辑。

- 如果需要，请修改名称。
- 点击蓝色加号按钮  以添加新设备。
- 点击以在 ASA 设备上执行以下操作。
  - 点击**编辑 (Edit)** 以修改现有的远程访问 VPN 配置。
  - 点击**删除 (Remove)**，从远程访问 VPN 配置中删除 ASA 设备。除组策略外，与该设备关联的所有连接配置文件和远程访问 VPN 设置都将被删除。您可以从对象页面中明确删除组策略。

    Note 如果 ASA 是唯一使用该配置的设备，则无法删除。或者，您可以删除远程访问 VPN 配置。

步骤 2 将配置更改从 CDO 部署到 ASA。

What to do next

您还可以通过键入配置或设备的名称来搜索远程访问 VPN 配置。

相关信息：

- 配置 ASA 远程访问 VPN 连接配置文件, on page 99。

配置 *ASA* 远程访问 *VPN* 连接配置文件

远程访问 VPN 连接配置文件定义了一些特征，这些特征允许外部用户使用 AnyConnect 客户端与系统创建 VPN 连接。每个配置文件都定义了用于用户身份验证的 AAA 服务器和证书、分配用户 IP 地址的地址池，以及定义各种面向用户的属性的组策略。

如果需要为不同的用户组提供不同的服务，或者有不同的身份验证源，您可以在远程访问 VPN 配置中创建多个配置文件。例如，如果您的组织与使用不同身份验证服务器的组织合并，您可以为使用这些身份验证服务器的新组创建配置文件。

远程访问 VPN 连接配置文件让您的用户可在外部网络（例如其家庭网络）上时连接到您的内部网络。创建单独的配置文件，以适应不同的身份验证方法。

开始之前

创建 ASA 远程访问 VPN 配置，第 95 页。

步骤 1 在 CDO 导航窗格中，点击**VPN** > **ASA/FDM 远程访问 VPN 配置 (ASA/FDM Remote Access VPN Configuration)**。您可以点击 VPN 配置以查看当前已配置多少连接配置文件和组策略的摘要信息。

注释 要了解分配给设备的组策略，请在操作中点击组策略。分配给连接配置文件的组策略会自动添加到列表中，并且无法删除。

如果您需要的组策略尚不存在，请点击  并从列表中进行选择。您可以创建其他组策略，以提供您所需的服务。请参阅创建 ASA 远程访问 VPN 组策略，第 89 页。

步骤 2 点击连接配置文件，然后在右侧边栏中的操作下点击添加连接配置文件。

步骤 3 配置基本连接属性。

- **连接配置文件名称 (Connection Profile Name)**：此连接的名称，最多 50 个字符，不能含空格。例如，MainOffice。

  注释 您在此输入的名称将是用户在 AnyConnect 客户端的连接列表中看到的名称。选择一个对您的用户来说有意义的名称。

- **组别名、组 URL (Group Alias, Group URL)**：别名包含特定连接配置文件的备用名称或 URL。在连接到 ASA 设备时，VPN 用户可以在连接列表中的 AnyConnect 客户端中选择别名。连接配置文件名称会自动添加为组别名。您还可以配置组 URL 列表，在发起远程访问 VPN 连接时您的终端可以从该列表中进行选择。如果用户使用组 URL 进行连接，系统将自动使用与 URL 匹配的连接配置文件。此 URL 供尚未安装 AnyConnect 客户端的客户使用。按需要添加组别名和 URL。在设备上定义的所有连接配置文件中，这些别名和 URL 必须是唯一的。组 URL 必须以 **https://** 开头。

- 例如，您可能有别名承包商和组 URLhttps://ravpn.example.com/contractor。安装 AnyConnect 客户端后，用户只需在连接的 AnyConnect VPN 下拉列表中选择组别名。

步骤 4 配置主身份源和辅助身份源（可选）。这些选项确定设备如何对远程用户进行身份验证，以启用远程访问 VPN 连接。最简单的方法是仅使用 AAA，然后选择 AD 领域或使用 LocalIdentitySource。根据**身份验证类型**，您可以使用以下方法：

- **仅 AAA (AAA Only)**：根据用户名和密码对用户进行身份验证和授权。有关详细信息，请参阅为连接配置文件配置 AAA ，第 100 页。
- **仅客户端证书 (Client Certificate Only)**：根据客户端设备身份证书进行用户身份验证。有关详细信息，请参阅为连接配置文件配置证书身份验证。
- **AAA 和 ClientCertificate (AAA and ClientCertificate)**：同时使用用户名/密码和客户端设备身份证书。

步骤 5 配置客户端的地址池。地址池定义了远程客户端在建立 VPN 连接时，系统可以分配给它们的 IP 地址。有关详细信息，请参阅配置客户端地址池分配。

步骤 6 点击**继续 (Continue)**。

步骤 7 从列表中选择要用于此配置文件的**组策略**，然后点击**选择 (Select)**。

组策略在建立隧道后设置用户连接的条款。系统包含名为“DfltGrpPolicy”的默认组策略。您可以创建其他组策略，以提供您所需的服务。请参阅创建 ASA 远程访问 VPN 组策略 ，第 89 页。

步骤 8 点击**继续 (Continue)**。

步骤 9 审核摘要。首先，验证摘要是否正确。您可以查看最终用户初步安装 AnyConnect 软件需要做什么，并测试他们是否可以完成 VPN 连接。点击  将这些说明复制到剪贴板，然后分发给您的用户。

步骤 10 点击**完成 (Done)**。

步骤 11 执行适用于 ASA 的端到端远程访问 VPN 配置过程的步骤 5。ASA 的端到端远程访问 VPN 配置过程 ，第 83 页

为连接配置文件配置 AAA

身份验证、授权和记账(AAA)服务器使用用户名和密码来确认是否允许用户访问远程访问VPN。如果使用 RADIUS 服务器，则可以区分已验证用户的授权级别，从而提供对受保护资源的差异化访问权限。还可以使用 RADIUS 记账服务来跟踪使用情况。

在配置AAA时，您必须配置主身份源。辅助源和备用源是可选的。如果想要实施双重身份验证，请使用辅助源，例如，RSA 令牌或 DUO。

主身份源选项

- **用户身份验证的主身份源 (Primary Identity Source for User Authentication)**：身份验证提供了一种识别用户的方法，这种方法通常先请用户输入有效用户名和有效密码，然后再授予访问权限。用于对远程用户进行身份验证的主身份源。必须在此源或可选的回退源中定义最终用户，才能完成 VPN 连接。选择以下一个选项：
  - Active Directory (AD) 身份领域。
  - RADIUS 服务器组。
  - LocalIdentitySource（本地用户数据库）：您可以直接在设备上定义用户，而不使用外部服务器。

    您可以点击身份源创建新的身份源。为 ASA 配置身份源, on page 84

- **回退本地身份源 (Fallback Local Identity Source)**：如果主要源是一个外部服务器，您可以选择LocalIdentitySource作为回退源，以防主服务器不可用。如果使用本地数据库作为回退源，请确保您定义的本地用户名/密码与外部服务器中的定义的用户名/密码相同。
- **删除选项 (Strip options)**：领域是管理域。启用以下选项将允许仅基于用户名进行身份验证。您可以启用这些选项的任意组合。但是，如果服务器无法分析分隔符，则必须选中这两个复选框。
  - **从用户名删除身份源服务器 (Strip Identity Source Server from Username)**：在将用户名传递到AAA服务器之前，是否要从用户名删除身份源名称。例如，如果选择此选项且用户输入域\用户名作为用户名，则该域将从用户名中删除，并发送到AAA服务器进行身份验证。默认情况下，此选项处于取消选中状态。
  - **从用户名删除组 (Strip Group from Username)**：在将用户名传递到 AAA 服务器之前，是否要从用户名删除组名称。此选项适用于 username@domain 格式中给定的名称；此选项会剥离域和 @ 符号。默认情况下，此选项处于取消选中状态。

辅助身份源

- **用于用户授权的辅助身份源 (Secondary Identity Source for User Authorization)**：可选的第二个身份源。如果用户成功使用主要源进行身份验证，则系统会提示其使用辅助源进行身份验证。可以选择 AD 领域、RADIUS 服务器组或本地身份源。
- **高级 (Advanced) 选项**：点击**高级 (Advanced)** 链接并配置以下选项：
  - **辅助源的备用本地身份源 (Fallback Local Identity Source for Secondary)**：如果辅助源为外部服务器，您可以选择LocalIdentitySource作为备用源，以防辅助服务器不可用。如果使用本地数据库作为备用源，请确保您定义的本地用户名/密码与辅助外部服务器中定义的用户名/密码相同。
  - **使用主要用户名进行辅助登录 (Use Primary Username for Secondary Login)**：默认情况下，使用辅助身份源时，系统将提示输入辅助源的用户名和密码。如果选择此选项，系统将仅提示您输入辅助密码，并使用与主身份源相同的用户名来进行辅助源身份验证。如果您在主身份源和辅助身份源中配置了相同的用户名，请选择此选项。
    - **会话服务器用户名 (Username for Session Server)**：身份验证成功后，用户名将显示在事件和统计控制面板中，用于确定基于用户或组的 SSL 解密和访问控制规则之间的匹配关系，并用于记账。由于使用了两个身份验证源，因此您需要告诉系统是使用主用户名还是辅助用户名作为用户身份。默认情况下，使用主用户名。
    - **密码类型 (Password Type)**：如何获取辅助服务器的密码。默认值为**提示**，这表明系统将提示用户输入密码。选择**主身份源密码**，自动使用用户在主服务器中进行身份验证时输入的密码。选择**公用密码**，为每个用户使用相同的密码，然后在**公用密码**字段中输入该密码。
  - **授权服务器 (Authorization Server)**：已配置为授权远程访问 VPN 用户的 RADIUS 服务器组。身份验证完成后，授权将控制对每个经过身份验证的用户都可用的服务和命令。授权通过组合一组描述用户被授权执行的操作、其实际功能和限制的属性来工作。如果您不使用授权，则单独的身份验证将为所有经过身份验证的用户提供相同的访问权限。

请注意，如果系统从 RADIUS 服务器获取的授权属性与组策略中定义的属性重叠，则 RADIUS 属性将覆盖组策略属性。

您可以点击创建 RADIUS 服务器组来创建新的服务器组。创建 ASA RADIUS 服务器对象或组, on page 87

- **记账服务器 (Accounting Server)**：（可选。）用于为远程访问 VPN 会话记账的 RADIUS 服务器组。记账会跟踪用户正在访问的服务以及他们正在使用的网络资源数量。ASA 设备向 RADIUS 服务器报告用户活动。记账信息包括每个会话的开始和停止时间、用户名、会话时通过设备的字节数、使用的服务以及每个会话的持续时间。然后，您可分析该数据，以进行网络管理、客户端计费或审核。您可以单独使用记账功能，也可以将其与身份验证和授权功能配合使用。

  您可以点击创建 RADIUS 服务器组来创建新的服务器组。创建 ASA RADIUS 服务器对象或组, on page 87

为连接配置文件配置证书身份验证

Note 此部分不适用于仅作为 AAA 的身份验证类型。

可以使用客户端设备安装的证书对远程访问 VPN 连接进行身份验证。

使用客户端证书时，仍可以配置辅助身份源、备用源，以及授权和记账服务器。这些是 AAA 选项；有关详细信息，请参阅配置 ASA 远程访问 VPN 连接配置文件, on page 99。

以下是证书特定的属性。您可以为主身份源和辅助身份源单独配置这些属性。配置辅助源为可选操作。

- **从证书中获取的用户名 (Username from Certificate)**：选择以下选项之一：
  - **映射特定字段 (Map Specific Field)**：按照**主要字段 (Primary Field)** 和**辅助字段 (Secondary Field)** 的顺序使用证书元素。默认值为 CN（公用名）和 OU（组织单位）。选择适用于您的组织的选项。这些字段组合在一起用于提供用户名，此名称用于事件和控制面板中，并出于匹配的目的，在 SSL 解密和访问控制规则中使用。
  - **使用完整 DN（可分辨名称）作为用户名 (Use entire DN [distinguished name] as username)**：系统自动从 DN 字段派生出用户名。
- 高级选项（不适用于作为仅客户端证书的身份验证类型）：点击高级链接并配置以下选项：
  - **在用户登录窗口预填证书中的用户名 (Prefill username from certificate on user login window)**：在提示用户进行身份验证时，是否在用户名字段填写检索到的用户名。
  - **在登录窗口隐藏用户名 (Hide username in login window)**：如果选择**预填充 (Prefill)** 选项，则可以隐藏用户名，这意味着用户无法编辑密码提示中的用户名。

配置客户端地址池分配

系统必须可以通过某种方法向连接到远程访问 VPN 的终端提供 IP 地址。AAA 服务器、DHCP 服务器、组策略中配置的 IP 地址池，或连接配置文件中配置的 IP 地址池可以提供这些地址。系统会按照以上顺序尝试使用这些资源，并在获取一个可用地址后停止尝试，然后将此地址分配给客户端。因此，您可以配置多个选项，以便在并发连接数异常多的情况下，可保障系统能获取地址。

使用下列一个或多个方法配置连接配置文件的地址池。

- IPv4 地址池和 IPv4 地址池：首先，创建最多六个指定子网的网络对象。可以为 IPv4 和 IPv6 单独配置池。然后，在组策略或者连接配置文件的 **IPv4 地址池 (IPv4 Address Pool)** 和 **IPv6 地址池 (IPv6 Address Pool)** 选项中，选择这些对象。无需同时配置 IPv4 和 IPv6，配置您想要支持的寻址方案即可。也不需要同时在组策略和连接配置文件中配置池。组策略会覆盖连接配置文件的设置，因此如果您在组策略中配置了池，则请将连接配置文件中的选项留空。请注意，系统按照您列出的顺序使用地址池。要创建新的 IPv4 地址池或新的 IPv6 地址池，请参阅创建 IP 地址池。
- **DHCP 服务器 (DHCP Servers)**：首先，使用一个或多个 IPv4 地址范围为远程访问 VPN 配置 DHCP 服务器（您无法使用 DHCP 配置 IPv6 池）。然后，使用 DHCP 服务器的 IP 地址创建主机网络对象。随后，便可以在连接配置文件的 **DHCP 服务器 (DHCP Servers)**属性中选择此对象。可以配置多个 DHCP 服务器。如果 DHCP 服务器有多个地址池，则可以在与连接配置文件关联的创建 ASA 远程访问 VPN 组策略中使用 **DHCP 作用域 (DHCP Scope)** 属性，选择要使用的池。使用池的网络地址创建主机网络对象。例如，如果 DHCP 池包含 192.168.15.0/24 和 192.168.16.0/24，将 DHCP 范围设置为 192.168.16.0 可确保从 192.168.16.0/24 子网中选择地址。

相关信息：

ASA 的端到端远程访问 VPN 配置过程

管理 *ASA* 设备上的 *AnyConnect* 软件包

您可以执行以下步骤之一，使用远程访问 VPN 向导上传 AnyConnect 软件包：

- 从 CDO 存储库上传软件包。
- 使用 HTTP、HTTPS、TFTP、FTP、SMB 或 SCP 协议从服务器上传数据包。

从 CDO 存储库上传 AnyConnect 软件包

远程访问 VPN 配置向导显示 CDO 存储库中每个操作系统的 AnyConnect 软件包，您可以从中选择并上传到设备。确保设备可以访问互联网并进行正确的 DNS 配置。

注释 如果所需的软件包在显示的列表中不可用，或者设备无法访问互联网，则可以使用预加载 AnyConnect 软件包的服务器上传软件包。

步骤 1 点击与操作系统对应的字段，然后选择 AnyConnect 软件包。

步骤 2 点击  以上传软件包。如果校验和不匹配，则 AnyConnect 软件包上传失败。您可以查看设备的工作流程选项卡，了解有关故障的更多详细信息。

从服务器将 AnyConnect 软件包上传到 ASA

将 AnyConnect 客户端软件包下载到您的计算机，并将其上传到可从 ASA 访问的远程服务器。稍后，使用 RA VPN 向导或 ASA 文件管理向导将 AnyConnect 软件包从该服务器上传到 ASA。必须在设备上为使用域名的 URL 正确配置 DNS。

ASA RA VPN 向导支持使用 HTTP、HTTPS、TFTP、FTP、SMB 或 SCP 协议上传数据包。

用于上传文件的受支持协议的语法：

协议	语法	示例
HTTP	http://[[path/]filename]	http://www.geonames.org/data-sources.html
HTTPS	https://[[path/]filename]	https://docs.aws.amazon.com/amazov/tagging.html
TFTP	tftp://[[path/]filename]	tftp://10.10.16.6/ftd/components.html
FTP	ftp://[user[:password]@]server[:port][/path/filename]	[illegible]
中小企业	smb://[[path/]filename]	smb://10.10.32.145//sambashare/hello.txt
SCP	scp://[[user[:password]@]server[/path]/filename]	scp://root:cisco123@10.10.10.166//root/events_send.py

Before you begin

请确保为所需的操作系统下载“AnyConnect 前端部署软件包”。始终下载最新的 AnyConnect 版本，以确保获得最新的功能、漏洞修复和安全补丁。请定期更新设备上的软件包。

Important 如果您选择使用 ASA 文件管理向导上传软件包，请不要在下载后修改软件包的名称。

Note 您可以为以下每个操作系统 (OS) 上传一个 AnyConnect 软件包：Windows、Mac 和 Linux。无法为特定操作系统类型上传多个版本。

步骤 1 从 https://software.cisco.com/download/home/283000185 下载 AnyConnect 软件包。

- 确保您接受 EULA 并具有 K9（加密映像）权限。
- 为您的操作系统选择“AnyConnect 前端部署软件包”。软件包名称类似于“anyconnect-win-4.7.04056-webdeploy-k9.pkg”。有适用于 Windows、macOS 和 Linux 的单独前端软件包。

步骤 2 将 AnyConnect 软件包上传到远程服务器。确保存在来自 ASA 设备和服务器的网络路由。

ASA RA VPN 向导支持上传数据包 HTTP、HTTPS、TFTP、FTP、SMB 或 SCP 协议。

Important 如果要将 AnyConnect 软件包上传到 HTTPS 服务器，请确保执行以下步骤：

- 在 ASA 设备上上传该服务器的受信任 CA 证书。
- 在 HTTPS 服务器上安装受信任的 CA 证书。

步骤 3 远程服务器的 URL 必须是不提示进行身份验证的直接链接。如果 URL 已进行预身份验证，则可以通过指定 RA VPN 向导的 URL 来下载文件。

步骤 4 如果远程服务器 IP 地址经过 NAT，则必须提供远程服务器位置的 NAT 公共 IP 地址。

将新的 AnyConnect 软件包上传到 ASA

您可以使用 RA VPN 向导或 ASA 文件管理向导将 AnyConnect 软件包上传到 ASA。

使用以下程序将新的 AnyConnect 软件包从 HTTP 或 HTTPS 服务器上传到 ASA 设备：

步骤 1 在**检测到的 AnyConnect 软件包 (AnyConnect Package Detected)** 中，您可以为 Windows、Mac 和 Linux 终端上传单独的软件包。

步骤 2 在相应的平台字段中，指定预上传与 Windows、Mac 和 Linux 兼容的 AnyConnect 软件包的服务器路径。服务器路径示例：'http://<ip_address> :port_number/<folder_name> /anyconnect-win-4.8.01090-webdeploy-k9.pkg', 'https:// :port_number/ /anyconnect-linux64-4.7.03052-webdeploy-k9.pkg'。

步骤 3 点击 以上传软件包。CDO 验证路径是否可访问，以及指定的文件名是否有效。验证成功后，系统将显示 AnyConnect 软件包的名称。当您将更多 ASA 设备添加到 RA VPN 配置时，您可以将 AnyConnect 软件包上传到这些设备。

步骤 4 点击**确定 (OK)**。AnyConnect 软件包已添加到 RA VPN 配置中。

步骤 5 从第 5 步开始创建 ASA 远程访问 VPN 配置。

What to do next

要完成 VPN 连接，您的用户必须在他们的工作站上安装 AnyConnect 客户端软件。有关详细信息，请参阅用户如何在 ASA 上安装 AnyConnect 客户端软件 。

使用文件管理向导上传 AnyConnect 软件包

使用文件管理向导将 AnyConnect 软件包从 HTTP、HTTPS、TFTP、FTP、SMB 或 SCP 服务器上传到单个或多个 ASA 设备。当您想要将 AnyConnect 软件包同时推送到多个 ASA 设备时，批量上传会派上用场。有关详细信息，请参阅 ASA 文件管理。

Important 如果您选择使用 ASA 文件管理向导上传软件包，请不要在下载后修改软件包的名称。

上传完成后，打开 ASA RA VPN 配置向导，您会注意到软件包已自动检测到。如果您为一个操作系统版本上传多个软件包，向导会在下拉列表中列出这些软件包，以便您从中选择一个。然后，您可以创建 RA VPN 配置并将其部署到设备。

替换现有的 AnyConnect 软件包

如果设备上已存在 AnyConnect 软件包，您可以在 RA VPN 向导中看到它们。您可以在下拉列表中查看操作系统的所有可用 AnyConnect 软件包。您可以从列表中选择现有软件包并将其替换为新软件包，但不能向列表中添加新软件包。

Note 如果要将现有软件包替换为新软件包，请确保已将新的 AnyConnect 软件包上传到 ASA 可以访问的网络上的服务器。

步骤 1 在左侧的 CDO 导航栏中，点击 VPN ASA/FDM Remote Access VPN。 >

步骤 2 选择要修改的 RA VPN 配置，然后在操作下点击编辑。

步骤 3 在“检测到的 AnyConnect 软件包”中，点击现有 AnyConnect 软件包旁边的图标。如果操作系统有多个版本的 AnyConnect 软件包，请从列表中选择要替换的软件包，然后点击编辑。现有软件包将从相应字段中消失。

步骤 4 指定预加载新 AnyConnect 软件包的服务器路径，然后点击 上传软件包。

步骤 5 点击**确定 (OK)**。新的 AnyConnect 软件包已添加到 RA VPN 配置中。

步骤 6 从步骤 6 开始继续创建 ASA 远程访问 VPN 配置, on page 95。

删除 AnyConnect 软件包

步骤 1 在左侧的 CDO 导航栏中，点击 VPN ASA/FDM Remote Access VPN。 >

步骤 2 选择要修改的 RA VPN 配置，然后在操作下点击编辑。

步骤 3 在“检测到的 AnyConnect 软件包”中，点击要删除的 AnyConnect 软件包旁边的图标。如果某个操作系统有多个版本的 AnyConnect 软件包，请从列表中选择要删除的软件包。现有软件包将从相应字段中消失。

Note 点击取消以停止删除操作并保留现有软件包，

步骤 4 点击**确定 (OK)**。设备的配置状态处于“未同步”状态。

Note 如果要在此阶段撤消删除操作，请转到**清单 (Inventory)** 页面，然后点击**放弃更改 (Discard Changes)** 以保留现有的 AnyConnect 软件包。

步骤 5 将配置更改从 CDO 部署到 ASA。

管理和部署预先存在的 ASA 远程访问 VPN 配置

当您载入已具有 RA VPN 设置的 ASDM 托管 ASA 设备时，它会发现并显示现有的远程访问 VPN 配置。CDO 会自动创建“默认 RA VPN 配置”，并将 ASA 设备与此配置相关联。有些 RA VPN 配置在 CDO 中无法读取或不受支持，但可以在 CDO 命令行界面中进行配置。

Note 本节未涵盖 CDO 中支持或不支持的每个配置。相反，它仅介绍最常用的内容。

要从已载入的 ASA 查看 RA VPN 配置，请执行以下步骤：

步骤 1 在 CDO 界面上，导航至 VPN ASA/FDM 远程访问 VPN 配置。 >

步骤 2 点击与载入的 ASA 设备对应的 RA VPN 配置。CDO 会自动创建“Default_RA_VPN_Configuration”并将 ASA 设备与此配置关联。您可以删除默认配置。在 CDO 中读取的 ASA RA VPN 配置分类如下：

- 设备设置
- 连接配置文件
- 组策略

设备设置

与载入的 ASA 设备关联的 RA VPN 配置显示在 Default_RA_VPN_Configuration 中。您需要点击此配置以查看与该配置关联的 ASA 设备的名称（在右侧的设备窗格中）。您还可以通过点击编辑按钮查看 ASA 设备中的 AnyConnect 软件包。

连接配置文件

CDO 支持并读取 ASA 设备的“AnyConnect 客户端 VPN 访问”中定义的连接配置文件。它不支持“无客户端 SSL VPN 访问”配置。

要查看连接配置文件属性，请执行以下步骤：

步骤 1 展开 **Default_RA_VPN_Configuration**。

步骤 2 点击所需的连接配置文件之一，然后点击**编辑**。

所有基本和高级 ASA RA VPN 属性都可以在 CDO RA VPN 配置页面的**连接配置文件名称和详细信息**中看到。

Note 您可以删除默认配置（选择默认的 RA VPN 配置，然后在右侧的**操作**窗格中点击**删除**）。

主身份源

- CDO 将 Connection Aliases 和 Group URLs 属性读取为 Group Alias 和 Group URL。

Note

- 系统不会读取配置了 SAML、多个证书和 AAA 以及多个证书的连接配置文件。
- 不支持具有接口和服务器组的身份验证服务器组。

- CDO 支持在主身份源中使用“AAA”、“AAA 和证书”和“仅证书”身份验证方法配置的 AnyConnect 连接配置文件。
- AAA 服务器组在 CDO 中被读取为主身份源中用户身份验证的主身份源（您可以通过选择 AAA 或 AAA 和客户端证书作为身份验证类型来查看此属性）。
  - 如果 AAA 服务器组配置的内容不是 LOCAL，则 CDO 会在主身份源下的“回退本地身份源”字段中读取并显示此属性。（您可以通过选择AAA作为身份验证类型来查看此属性）。

    要了解有关 CDO 中读取的服务器组属性的详细信息，请参阅 AAA 服务器组。

辅助身份源

辅助身份源显示 ASA 设备的辅助身份验证属性。要查看这些属性，请选择 AAA 或 AAA 和客户端证书作为身份验证类型，然后点击查看辅助身份源。

- 用户身份验证的辅助身份源显示辅助身份验证服务器组属性。
  - 如果服务器组配置的内容不是 LOCAL，则 CDO 会在“辅助身份源”下的“备用本地身份源”字段中读取并显示此属性。
- CDO 不支持 Attribute Server 和 Interface-Specific Authorization Server Groups 属性。

要了解有关 CDO 中读取的服务器组属性的详细信息，请参阅 AAA 服务器组。

授权服务器

- 授权服务器显示授权服务器组属性。
- CDO 不支持具有接口和服务器组的授权服务器组。

要了解有关 CDO 中读取的 RADIUS 服务器组属性的详细信息，请参阅 RADIUS 服务器组。

审计服务器

记帐服务器显示记帐服务器组属性。要了解有关 CDO 中读取的服务器组属性的详细信息，请参阅 RADIUS 服务器组。

客户端地址池分配

CDO 会将**客户端地址分配属性**（**DHCP 服务器**、**客户端地址池**和**客户端 IPv6 地址池**）作为对象进行读取。（您可以在客户端地址池分配中查看这些属性）。DHCP服务器详细信息以文字形式读取。

Note CDO 不支持在特定接口上分配 IP 地址池。但是，可以在 ASA 命令行界面 (CLI) 中看到这些属性。

AAA 服务器组

CDO 将 LDAP 服务器组及其关联的 LDAP 服务器表示为 Active Directory 领域对象。对于 Active Directory (AD)，领域就等于 Active Directory 域。请注意，CDO 会读取已经存在的 AD 领域对象的 AD 密码。

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > ASA 对象 (ASA Objects)**。

步骤 2 应用 Active Directory 领域过滤器以查看此对象。

步骤 3 选择所需的 Active Directory 领域对象，然后点击编辑以查看其详细信息。

What to do next

可以看到 AD 领域包含关联的 AD 服务器及其配置。如果 AD 领域有多个 Active Directory (AD) 服务器，则 AD 服务器需要彼此重复，并支持相同的 AD 域。因此，与该 AD 领域关联的所有 AD 服务器的基本领域属性（例如目录名称、目录密码和基本可分辨名称）必须相同。如果这些属性不同，CDO 会在 Active Directory 领域对象中显示警告消息。您必须更正这些属性，使它们在所有 AD 服务器之间保持一致。如果继续而不解决此警告，CDO 将使用其中一个 AD 服务器属性并将其应用于该领域对象中的其他服务器。

RADIUS 服务器组

ASA 设备的 AAA RADIUS 服务器组属性在 CDO 中作为 RADIUS 服务器组对象读取。

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > ASA 对象 (ASA Objects)**。

步骤 2 应用 RADIUS 服务器组过滤器以查看此对象。

步骤 3 选择所需的对象，然后点击编辑以查看其详细信息。

- 在 ASA 中启用动态授权在 CDO 中读取为动态授权（仅适用于 RA VPN）。
- 重新激活模式下的耗尽选项在 CDO 中读取，因此与耗尽时间关联的死区时间值在 CDO 中读取。但是，不会在 CDO 中读取 Timed 属性。
- CDO 不支持记账模式、定时、启用临时记账更新、启用临时记账更新和仅使用授权模式。

RADIUS 服务器

当 CDO 从 ASA 读取 Radius 服务器时，它会创建一个 Radius 服务器对象，该对象将名称指定为“Radius 服务器组名称或 IP 地址”。

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > ASA 对象 (ASA Objects)**。

步骤 2 应用 RADIUS 服务器过滤器以查看此对象。

步骤 3 选择所需的对象，然后点击编辑以查看其详细信息。

组策略

在**组策略 (Group Policy)** 部分中，点击下拉列表以查看与设备关联的组策略。

Attention CDO 将使用隧道协议配置的组策略读取为 **SSL VPN 客户端**。

CDO 读取 ASA 中配置的大多数组策略属性。该信息显示在 RA VPN 组策略向导中的选项卡中。要查看从 ASA 设备读取的组策略的详细信息，您需要执行以下操作：

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FTD 网络对象 (FTD Network Objects)**。

步骤 2 **RA VPN 组策略**的过滤器。

步骤 3 选择与该设备关联的组策略，然后点击**编辑 (Edit)**。

What to do next

Note CDO 不支持 ASA 设备的分割隧道中定义的标准访问控制列表 (ACL)。它支持扩展访问控制列表 (ACL) 并将其作为 ACL 读取到 ASA 策略中。有关详细信息，请参阅ASA 远程访问 VPN 组策略属性。要查看策略，可以在导航栏上点击**策略 (Policies)** > **ASA 访问策略 (ASA Access Policies)**。

要选择扩展 ACL，请执行以下操作：

- 点击**拆分隧道 (Split Tunneling)** 选项卡。
- 根据 ASA 中的流量是使用 IPv4 还是 IPv6 地址，从相应的下拉列表中选择“允许指定的流量通过隧道”(Allow specified traffic over tunnel) 或“排除下面指定的网络”(Exclude networks specified below)。选择从 ASA 导入的扩展 ACL。

创建 IP 地址池

您可以为 ASA 配置 IPv4 和 IPv6 IP 地址池，以将其分配给使用 VPN 连接远程连接到您的网络的客户端。地址池的指定顺序非常重要。如果为连接配置文件或组策略配置了多个地址池，则ASA将按您向 ASA 添加地址池的顺序使用地址池。

要定义 IPv4 地址池，请提供 IP 地址范围。IPv4 地址池的一个示例是 10.10.147.100 - 10.10.147.177。

定义 IPv6 地址池时，需要提供起始地址范围、地址前缀和地址池可配置的地址数量。IPv6 地址池的一个示例是 2001:DB8:1::1。

如果从非本地子网分配地址，我们建议添加位于子网边界的地址池，从而可更轻松地添加这些网络的路由。

执行以下操作以创建 IP 地址池：

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > ASA 对象 (ASA Objects)**。

步骤 2 点击蓝色加号按钮  ，然后选择 **ASA** > **地址池 (Address Pool)**。

步骤 3 在**创建 IP 地址池 (Create IP Address Pool)** 对话框中输入以下信息：

- **对象名称 (Object Name)**：输入地址池的名称。最多可包含 64 个字符
- **IPv4 地址池 (IPv4 address pool)**：选择此单选按钮可配置 IPv4 地址池。
  - **IPv4 地址范围 (IPv4 Address Range)**：输入每个配置的池中可用的第一个 IP 地址和最后一个 IP 地址。例如，10.10.147.100 - 10.10.147.177。
  - **掩码 (Mask)**：标识此 IP 地址池所属的子网。
- **IPv6 地址池 (IPv6 address pool)**：选择此单选按钮可配置 IPv6 地址池。
  - **IPv6 地址**：输入配置的池中可用的第一个 IP 地址和前缀长度（以位为单位）。 <address>/<prefix> 格式。例如，2001:DB8:1::1/3。
  - **地址数量 (Number of Addresses)**：标识地址池中从开始 IP 地址开始的 IPv6 地址的数量。

步骤 4 点击**保存 (Save)**。

远程访问 VPN 基于证书的身份验证

在以下情况下，远程访问 VPN 使用数字证书对安全网关和 AnyConnect 客户端（终端）进行身份验证：

重要事项 CDO 处理 VPN 头端 (ASA) 上的数字证书安装。它不处理 AnyConnect 客户端设备上的证书安装。您的组织的管理员必须处理此问题。

- 识别和认证 VPN 前端设备 (ASA)：

当 AnyConnect 客户端请求 VPN 连接时，VPN 头端需要身份证书来识别和认证自己。使用 CDO，您必须在设备上安装身份证书。请参阅使用 PKCS12 或证书和密钥安装身份证书。不强制要求在 AnyConnect 客户端上安装颁发机构的 CA 证书。

从 CDO 创建远程访问 VPN 配置时，将注册的身份证书分配给设备的外部接口，并将配置下载到设备。身份证书在设备的外部接口上完全可操作。

当 AnyConnect 客户端尝试连接到 VPN 时，设备通过向 AnyConnect 客户端提供其身份证书来对自身进行身份验证。AnyConnect 客户端使用其受信任的 CA 证书验证此身份证书，并信任该证书，从而信任设备。如果 CA 证书未安装在 AnyConnect 客户端上，则用户必须在系统提示时手动信任设备。

- 识别和认证 AnyConnect 客户端：

注释 当您在 RA VPN 配置的连接配置文件中使用“仅客户端证书”或“AAA 和客户端证书”作为身份验证方法时，这适用。它不适用于“仅 AAA”。

设备受信任后，AnyConnect 客户端需要对自身进行身份验证才能完成 VPN 连接。您必须在 AnyConnect 客户端上安装身份证书，并使用 CDO 在设备上安装受信任的 CA 证书。这些证书必须由同一证书颁发机构颁发。请参阅在 ASA 中安装受信任的 CA 证书。

AnyConnect 客户端提供其身份证书，设备使用其受信任的 CA 证书验证此证书并建立 VPN 连接。

从 NAT 豁免远程访问流量

配置 NAT 免除，使进出远程访问 VPN 终端的流量免于执行 NAT 转换。如果不豁免 VPN 流量执行 NAT，请确保外部和内部接口的现有 NAT 规则不适用于 RA VPN 地址池。NAT 豁免规则是给定源/目标接口和网络组合的手动静态身份 NAT 规则，但它们不会反映在 NAT 策略中，它们是隐藏起来的。如果启用 NAT 豁免，还必须进行以下配置。

- **内部接口**：选择远程用户将要访问的内部网络的接口。所创建的 NAT 规则用于这些接口。
- **内部网络**：选择代表远程用户将访问的内部网络的网络对象。网络列表必须包含与您支持的地址池相同的 IP 类型。

开始之前

创建与该设备的连接配置文件和组策略中使用的本地 IP 地址池的配置相匹配的 ASA 网络对象。配置 NAT 规则时，必须将这些网络对象分配为目的地址和转换后的地址。请参阅创建 ASA 网络对象。

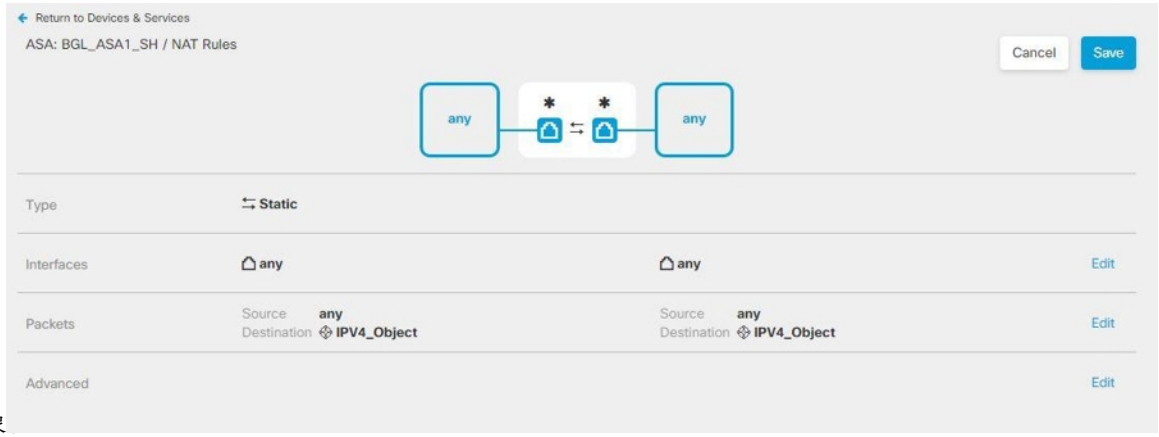
步骤 1 在 CDO 导航栏中，点击**清单 (Inventory)**。

步骤 2 使用**清单 (Inventory)** 过滤器和搜索字段查找要为其创建 NAT 规则的 ASA 设备。

步骤 3 在详细信息面板的**管理 (Management)** 区域中，点击 **NAT** NAT。

步骤 4 点击 + > **两次 NAT (Twice NAT)**。

1. 在第 1 部分中，选择**静态 (Static)**。点击**继续**。
2. 在第 2 部分中，选择**源接口 (Source Interface)** = 'any' 以及**目标接口 (Destination Interface)** = 'any'。点击**继续 (Continue)**。
3. 在第 3 部分中，选择**源接口地址 (Source Original Address)** = 'any' 以及**源转换地址 (Source Translated Address)** = 'any'。
4. 选择**使用目标 (Use Destination)**。
   1. **目标原始地址 (Destination Original Address)** 和**源转换地址 (Source Translated Address)**：点击下拉列表中的**选择 (Choose)**，然后选择与本地 IP 地址池的配置匹配的网络对象。在下面的示例中，“IPV4_Object”是与 ASA (BGL_ASA1_SH) 设备的连接配置文件和组策略设置中使用的 IPv4 地址池对象具有相同配置的网络对象



   2. 选择**为传入数据包禁用代理 ARP (Disable proxy ARP for incoming packets)**。
   3. 点击**保存 (Save)**。
   4. 重复此过程（从步骤 4 开始），为与 IP 地址池等效的每个其他网络对象创建等效规则。

步骤 5 将配置更改从 CDO 部署到 ASA。

用户如何在 ASA 上安装 AnyConnect 客户端软件

要完成 VPN 连接，您的用户必须安装 AnyConnect 客户端软件。可以使用现有的软件分发方法直接安装该软件。或者，可以让用户直接从 ASA 设备安装 AnyConnect 客户端。

Note 用户必须对其工作站具有管理员权限才能安装软件。

如果您决定让用户一开始从 ASA 设备安装软件，请告知用户执行以下步骤。

Note Android 和 iOS 用户应从相应的应用商店下载 AnyConnect。

步骤 1 使用 Web 浏览器，打开 **https://***ravpn-address*，其中 *ravpn-address* 是您允许 VPN 连接的外部接口的 IP 地址或主机名。您在配置远程访问 VPN 时确定此接口。系统提示用户登录。

步骤 2 登录到网站。用户使用为远程访问 VPN 配置的目录服务器进行身份验证。登录成功后可继续操作。如果登录成功，系统将确定用户是否已具有所需的 AnyConnect 客户端版本。如果用户的计算机上没有 AnyConnect 客户端，或者客户端的版本较低，系统将自动开始安装 AnyConnect 软件。安装后，AnyConnect 会完成远程访问 VPN 连接。

修改 ASA 远程访问 VPN 配置

当 ASA 设备载入 CDO 时，它会发现并显示来自载入的 ASA 设备的原有远程访问 VPN 配置。有关详细信息，请参阅管理和部署预先存在的 ASA 远程访问 VPN 配置，第 107 页。

您可以修改这些配置并将新配置下载到设备。

- 修改 ASA 远程访问 VPN 配置
- 修改 ASA 连接配置文件

修改远程访问 *VPN* 配置

步骤 1 在左侧的 CDO 导航栏中，点击 VPN > 远程访问 VPN 配置。

步骤 2 如果要在 VPN 配置中添加或删除组策略，请点击与载入的 ASA 设备关联的 VPN 配置。在左侧的操作窗格中，点击组策略。

a) 点击蓝色 + 图标并配置选择，然后点击选择。

b) 点击“保存”(Save)。您还可以创建 ASA 远程访问 VPN 组策略。

步骤 3 点击 VPN 配置，然后在左侧的操作窗格中，点击编辑。

向导将列出与配置关联的 ASA 设备。

a) 您可以按照与创建时相同的方式修改以下详细信息：

- 更改远程访问 VPN 配置的名称。
- 点击显示设备详细信息的行中显示的三个点，然后点击编辑。

有关详细信息，请参阅创建 ASA 远程访问 VPN 配置，第 95 页

步骤 4 点击**确定**。

步骤 5 预览和部署所有设备的配置更改，第 160 页

修改 *ASA* 连接配置文件

步骤 1 在左侧的 CDO 导航栏中，点击 VPN > 远程访问 VPN 配置。

步骤 2 展开与载入的 ASA 设备关联的 VPN 配置，并选择连接配置文件。

步骤 3 在左侧的**操作 (Actions)** 窗格中，点击**编辑 (Edit)**。

步骤 4 以与创建时相同的方式编辑值，然后点击完成。

有关详细信息，请参阅配置 ASA 远程访问 VPN 连接配置文件，第 99 页

步骤 5 预览和部署所有设备的配置更改，第 160 页

上传 RA AnyConnect 客户端配置文件

远程访问 VPN AnyConnect 客户端配置文件是存储在文件中的一组配置参数。这些不同的 AnyConnect 客户端配置文件包含核心客户端 VPN 功能和可选客户端模块网络访问管理器、AMP 启动器、ISE 终端安全评估、网络可视性、客户体验反馈、Umbrella 漫游安全和网络安全的配置设置。

CDO 允许将这些配置文件作为对象上传，以便稍后在组策略中使用。

- **AnyConnect VPN 配置文件 (AnyConnect VPN Profile)** - AnyConnect 客户端配置文件随 AnyConnect 客户端软件一起下载到客户端。这些配置文件定义与客户端相关的诸多选项，例如启动时自动连接和自动重新连接，以及最终用户是否可以更改 AnyConnect 客户端首选项和高级设置中的选项。CDO 支持 XML 文件格式。
- **AMP 启用程序服务配置文件 (AMP Enabler Service Profile)** - 该配置文件用于 AnyConnect AMP 启用程序。当远程访问 VPN 用户连接到 VPN 时，AMP 启动器和此配置文件会从 FDM 管理 设备推送到终端。CDO 支持 XML 和 ASP 文件格式。
- **反馈配置文件 (Feedback Profile)** - 您可以添加客户体验反馈配置文件并选择此类型，以接收有关客户已启用和使用的功能和模块的信息。CDO 支持 FSP 文件格式。
- **ISE 终端安全评估配置文件 (ISE Posture Profile)** - 如果要为 AnyConnect ISE 终端安全评估模块添加配置文件，请选择此选项。CDO 支持 XML 和 ISP 文件格式。
- **网络访问管理器服务配置文件 (Network Access Manager Service Profile)** - 使用网络访问管理器配置文件编辑器配置和添加 NAM 配置文件。CDO 支持 XML 和 NSP 文件格式。
- **网络可视性服务配置文件 (Network Access Manager Service Profile)** - AnyConnect 网络可视性模块的配置文件。您可以使用 NVM 配置文件编辑器创建配置文件。CDO 支持 XML 和 NVMSP 文件格式。
- **Umbrella 漫游安全配置文件 (Umbrella Roaming Security Profile)** - 如果部署 Umbrella 漫游安全模块，则必须选择此文件类型。CDO 支持 XML 和 JSON 文件格式。
- **网络安全服务配置文件 (Web Security Service Profile)** - 在为网络安全模块添加配置文件时选择此文件类型。CDO 支持 XML、WSO 和 WSP 文件格式。

Before you begin

使用适当的基于 GUI AnyConnect 配置文件编辑器创建所需的配置文件。您可以从思科软件下载中心的 AnyConnect 安全移动客户端类别下载配置文件编辑器，并安装 AnyConnect“配置文件编辑器 - Windows/独立安装程序 (MSI)”(Profile Editor - Windows / Standalone installer [MSI])。配置文件编辑器安装程序包含独立版本的配置文件编辑器。此安装文件仅适用于 Windows，文件名为 anyconnect-profileeditor-win-<version>-k9.msi，其中 <version> 指 AnyConnect 版本。例如，

anyconnect-profileeditor-win-4.3.04027-k9.msi。您还必须在安装配置文件编辑器之前安装 Java JRE 1.6（或更高版本）。

除 Umbrella 漫游安全配置文件编辑器外，此软件包包含创建模块所需的所有配置文件编辑器。有关详细信息，请参阅相应版本的《思科 AnyConnect 安全移动客户端管理员指南》中的 *AnyConnect* 配置文件编辑器一章。从 Umbrella 控制面板单独下载 Umbrella 漫游安全配置文件。有关详细信息，请参阅《思科 Umbrella 用户指南》中“Umbrella 漫游安全”一章的“从 Umbrella 控制面板下载 AnyConnect 漫游安全配置文件”部分。

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击“加号”  按钮。

步骤 3 点击 **RA VPN 对象（ASA 和 FDM）(RA VPN Objects [ASA & FDM])** > **AnyConnect 客户端配置文件 (AnyConnect Client Profile)**。

步骤 4 在**对象名称 (Object Name)** 字段中输入 AnyConnect 客户端配置文件名称。

步骤 5 点击**浏览 (Browse)** 并选择使用配置文件编辑器创建的文件。

步骤 6 点击**打开**上传配置文件。

步骤 7 点击**添加 (Add)** 以添加对象。

相关信息：

- 将客户端模块与 RA VPN 组策略窗口中的 AnyConnect VPN 配置文件关联。请参阅创建 ASA 远程访问 VPN 组策略 。

Note 所有 ASA 版本和运行软件版本 6.7 或更高版本的 FDM 都支持客户端模块关联。

验证 ASA 的远程访问 VPN 配置

在配置远程访问 VPN 并将该配置部署到设备后，请确认是否可以进行远程连接。

步骤 1 在外部网络中，使用 AnyConnect 客户端建立 VPN 连接。使用 Web 浏览器，打开 **https://***ravpn-address*，其中 *ravpn-address* 是您允许 VPN 连接的外部接口的 IP 地址或主机名。如有必要，安装客户端软件并完成连接。请参阅用户如何在 ASA 上安装 AnyConnect 客户端软件 。如果配置了组 URL，也可尝试这些 URL。

步骤 2 在**清单 (Inventory)** 页面中，选择要验证的设备（FTD 或 ASA），然后点击**设备操作 (Device Actions)** 下的**命令行接口 (Command Line Interface)**。

步骤 3 使用 **show vpn-sessiondb** 命令可查看有关当前 VPN 会话的摘要信息。

步骤 4 统计信息应显示您的活动 AnyConnect 客户端会话以及有关累积会话、峰值并发会话数量和非活动会话的信息。以下是该命令的输出示例。

```
> show vpn-sessiondb
--------------------------------------------------------------------------------
VPN Session Summary
--------------------------------------------------------------------------------
                            Active : Cumulative : Peak Concur : Inactive
                           ------------------------------------------------
AnyConnect Client           :      1 :         49 :           3 :        0
  SSL/TLS/DTLS              :      1 :         49 :           3 :        0
Clientless VPN              :      0 :          1 :           1
  Browser                   :      0 :          1 :           1
--------------------------------------------------------------------------------


   Total Active and Inactive    :      1             Total Cumulative :     50
   Device Total VPN Capacity    :  10000
   Device Load                  :     0%
   --------------------------------------------------------------------------------

   --------------------------------------------------------------------------------
   Tunnels Summary
   --------------------------------------------------------------------------------
                                 Active : Cumulative : Peak Concurrent
                                ------------------------------------------------
   Clientless                   :      0 :          1 :               1
   AnyConnect-Parent            :      1 :         49 :               3
   SSL-Tunnel                   :      1 :         46 :               3
   DTLS-Tunnel                  :      1 :         46 :               3
   --------------------------------------------------------------------------------
   Totals                       :      3 :        142
   --------------------------------------------------------------------------------

   --------------------------------------------------------------------------------
   IPv6 Usage Summary
   --------------------------------------------------------------------------------
                                 Active : Cumulative : Peak Concurrent
                                ------------------------------------------------
   AnyConnect SSL/TLS/DTLS      :        :           :
     Tunneled IPv6              :      1 :         20 :           2
   --------------------------------------------------------------------------------
```

步骤 5 使用 **show vpn-sessiondb anyconnect** 命令可查看有关当前 AnyConnect VPN 会话的详细信息。详细信息包括使用的加密方式、传输和接收的字节数及其他统计信息。如果使用 VPN 连接，随着您重新发出命令，您应可看到传输/接收的字节数会变化。

步骤 6 使用 **show vpn-sessiondb anyconnect** 命令可查看有关当前 AnyConnect VPN 会话的详细信息。详细信息包括使用的加密方式、传输和接收的字节数及其他统计信息。如果使用 VPN 连接，随着您重新发出命令，您应可看到传输/接收的字节数会变化。

```
> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : User1                  Index        : 4820
Assigned IP  : 172.18.0.1             Public IP    : 192.168.2.20
Assigned IPv6: 2009::1
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 27731                  Bytes Rx     : 14427
Group Policy : MyRaVpn|Policy         Tunnel Group : MyRaVpn
Login Time   : 21:58:10 UTC Mon Apr 10 2017
Duration     : 0h:51m:13s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a800fd012d400058ebfff2
Security Grp : none                   Tunnel Zone : 0
```

查看 ASA 的远程访问 VPN 配置详细信息

步骤 1 在左侧的 CDO 导航栏中，点击 **VPN** > **ASA/FDM 远程访问 VPN 配置**。

步骤 2 点击现有的 VPN 配置对象。该组显示有关当前已配置多少连接配置文件和组策略的摘要信息。

- 展开 RA VPN 配置以查看与其关联的所有连接配置文件。
  - 点击添加 + 按钮可添加新的连接配置文件。
  - 点击查看按钮 ( )，打开连接配置文件和连接说明的摘要。在操作下，您可以点击编辑以修改更改。
- 您可以点击“操作”下的以下选项之一来执行其他任务：
  - 点击组策略以分配/添加组策略。
  - 点击不再需要的配置对象或连接配置文件，然后点击删除进行删除。

监控远程访问虚拟专用网络会话

远程访问虚拟专用网络 (RA VPN) 为远程用户（如移动用户或远程工作者）提供安全连接。监控这些连接可以让连接和用户会话性能的重要指标变得一目了然。Cisco Defense Orchestrator (CDO) RA VPN 监控功能使您能够快速确定远程访问 VPN 问题是否存在及其存在的位置。然后，您可以应用这些知识并使用网络管理工具来减少或消除网络和用户问题。您还可以根据需要断开远程访问 VPN 会话。

“远程访问虚拟专用监控”(Remote Access Virtual Private Monitoring) 页面提供以下信息：

- 长达一年的活动会话和历史会话列表。
- 显示直观的图形视觉效果，让 CDO 管理的所有活动 VPN 前端变得一目了然。
- 实时会话屏幕会显示 CDO 租户中最常用的操作系统和 VPN 连接配置文件。它还会显示平均会话持续时间以及上传和下载的数据。
- 过滤功能可根据设备类型、设备名称、会话长度以及传输和接收的数据量等条件来缩小搜索范围。

相关信息：

- 监控实时 AnyConnect RA VPN 会话, on page 119
- 监控历史 AnyConnect RA VPN 会话, on page 120
- 搜索和过滤 RA VPN 会话
- 自定义 RA VPN 监控视图
- 将 RA VPN 会话导出至 CSV 文件
- 断开用户的所有活动 RA VPN 会话

监控实时 AnyConnect RA VPN 会话

您可以监控设备上活动 AnyConnect RA VPN 会话的实时数据。这些数据每 10 分钟会自动刷新一次。如果要随时检索最新的会话列表，请点击屏幕右上角显示的重新加载图标 。

开始之前

- 将 RA VPN 前端载入 CDO。
- 确保要监控实时数据的设备的连接状态在**清单 (Inventory)** 页面上为“在线”(Online)。

步骤 1 在 CDO 导航窗格中，点击 **VPN** > **远程访问 VPN 监控**。

或者，您可以点击 CDO 主页上的**查看活动远程访问 VPN 会话 (View Active Remote Access VPN Sessions)**，或导航至 **VPN** > **远程访问 VPN (Remote Access VPN)**并点击屏幕右上角的 图标。

步骤 2 点击 **RA VPN**。

步骤 3 点击**实时 (Live)**。

您可以搜索和过滤 RA VPN 会话以根据设备类型、会话长度以及上传和下载数据范围等条件来缩小搜索范围。

注释 **数据 TX** 和**数据 RX** 信息不适用于 FTD。

查看实时数据

实时数据以控制面板和表格形式显示。

面板视图

您必须点击屏幕右上角的**显示图表视图**图标才能查看控制面板。

控制面板提供 CDO 管理的所有活动 VPN 头端的概览视图。

- **明细（所有设备）**：显示实时会话总数。它还显示了一个分为四个弧长的饼形图。它说明会话数最多的前三台设备的 VPN 会话百分比。剩余的弧长表示其他设备的总和。
- 显示 CDO 租户中最常用的操作系统和 VPN 连接配置文件。
- 显示平均会话持续时间以及上传和下载的数据。
- **按国家/地区排列的活动会话 (Active Sessions by Country)**：显示连接到 RA VPN 前端的用户的位置的交互式热度地图。
  - 用户已连接的国家/地区以逐渐变深的蓝色显示，具体取决于从该国家/地区建立的会话的相对比例 - 蓝色越深表示从该国家/地区建立的会话越多。
  - 地图底部的图例提供了一个比例，表示某个国家/地区的会话数与其所用蓝色阴影之间的相关性。

- 将鼠标指针悬停在地图上，可查看国家/地区名称以及从该国家/地区建立的活动用户会话总数。
- 将鼠标指针悬停在表格上，可在地图上看到国家/地区的位置和活动用户会话总数。

表格视图

点击屏幕右上角的**显示表格视图**图标，以表格格式查看数据。

表格形式提供当前连接的 VPN 用户的完整列表。

- “位置”列通过对公共 IP 地址进行地理定位来显示连接到 VPN 头端的所有用户的位置。点击一行可查看用户详细信息。点击左侧窗格中的位置链接时，用户的位置会显示在 Google 地图上。

重要事项 CDO 对实时数据应用标准过滤器，并在控制面板上显示这些数据。仅当显示表格数据时，才能应用新过滤器，因为可视化控制面板视图中不支持自定义过滤器。点击**清除**以删除已应用的所有过滤器。您无法删除标准过滤器。

您可以使用搜索和过滤 RA VPN 会话功能根据设备类型、会话长度以及上传和下载数据范围等条件来缩小搜索范围。请注意，一次最多可以显示 10,000 个结果。

状态列中带有活动标签的绿点表示活动 VPN 用户的会话。

监控历史 AnyConnect RA VPN 会话

您可以监控过去三个月内记录的 AnyConnect RA VPN 会话的历史数据。

开始之前

- 将 RA VPN 前端载入 CDO。

步骤 1 在 CDO 导航窗格中，点击 **VPN** > **远程访问 VPN 监控**。

或者，您可以点击 CDO 主页上的**查看活动远程访问 VPN 会话 (View Active Remote Access VPN Sessions)**，或导航至 **VPN** > **远程访问 VPN (Remote Access VPN)** 并点击右上角的 图标。

步骤 2 点击 **RA VPN**。

步骤 3 点击**历史 (Historical)**。

CDO 会显示过去三个月内记录的 RA VPN 会话的历史数据。

您可以使用搜索和过滤 RA VPN 会话功能根据设备类型、会话长度以及上传和下载数据范围等条件来缩小搜索范围。

数据 TX 和**数据 RX** 信息不适用于 FTD。

查看历史数据

历史数据以控制面板和表格形式显示。

面板视图

您必须点击屏幕右上角的“显示图表视图”图标才能查看控制面板。您将看到控制面板视图和表格视图。

控制面板提供 CDO 管理的所有活动 VPN 头端的概览视图。它会提供一个条形图，以便显示过去 24 小时、7 天和 30 天内为所有设备记录的 VPN 会话。您可以从下拉列表中选择持续时间。您可以将鼠标悬停在各个条形上，以查看当天的日期和会话总数。

表格视图

您必须点击屏幕右上角显示的“显示表格视图”图标，才能仅查看表格视图。此表格提供了过去三个月内连接的 VPN 用户的完整列表。

“位置”列通过对公共 IP 地址进行地理定位来显示连接到 VPN 头端的所有用户的位置。点击一行可查看用户详细信息。点击左侧窗格中的位置链接时，用户的位置会显示在 Google 地图上。

重要事项 CDO 对历史数据应用标准过滤器，并将其显示在控制面板上。您只能在显示表格数据时应用新过滤器，因为自定义过滤器不支持控制面板。清除新应用的过滤器会重新启动控制面板（在屏幕上，点击清除可删除手动应用的过滤器）。您无法删除标准过滤器。

您可以使用搜索和过滤 RA VPN 会话功能根据会话日期和时间范围、会话长度以及上传和下载数据范围等条件来缩小搜索范围。请注意，一次最多可以显示 10,000 个结果。

状态列中带有活动标签的绿点表示活动 VPN 用户的会话。

搜索和过滤 RA VPN 会话

搜索

使用搜索栏功能查找 RA VPN 会话。开始在搜索栏中键入设备名称、IP 地址或序列号，系统将显示符合搜索条件的 RA VPN 会话。搜索不区分大小写。

过滤

使用过滤器边栏可根据会话时间范围、会话长度以及上传和下载数据范围等条件查找 RA VPN 会话。过滤功能可用于实时视图和历史视图。

- **按设备过滤 (Filter by Devices)**：从**所有类型 (All Types)** 选项卡中选择一个或所有设备以查看所选设备的会话。该窗口还会根据设备的类型来对它们进行分类，并在相应的选项卡下显示它们。

- **会话时间范围 (Sessions Time Range)**（仅适用于历史数据）：查看指定日期和时间范围内的历史会话。请注意，您可以查看过去三个月内记录的数据。
- **会话长度 (Sessions Length)**：根据指定会话的持续时间长度查看会话。设置时间单位（小时、分钟或秒），并通过移动滑块指定最小和最大持续时间。您还可以在提供的字段中指定长度。
- **上传 (TX) (Upload [TX])**：根据上传或传输到安全网络的指定数据量查看会话。设置单位（GB、MB 或 KB），并通过相应地移动滑块来选择范围。您还可以在可用字段中指定值。
- **下载 (RX) (Download [RX])**：根据从安全网络下载或接收的指定数据量查看会话。设置单位（GB、MB 或 KB），并通过相应地移动滑块来选择范围。您还可以在可用字段中指定值。

自定义 RA VPN 监控视图

您可以在实时和历史模式下修改 RA VPN 监控视图，以仅包含适用于所需视图的列标题。点击列右侧的列过滤器图标  ，然后选择或取消选择所需的列。

CDO 会在您下次登录 CDO 时记住您的选择。

将 RA VPN 会话导出至 CSV 文件

您可以将一个或多个设备的 RA VPN 会话导出至以逗号来分隔值的 (.csv) 文件。您可以在电子表格应用（例如 Microsoft Excel）中打开 .csv 文件，对列表中的项目进行排序和过滤。这些信息可帮助您分析 RA VPN 会话。每次导出会话时，CDO 都会创建一个新的 .csv 文件，其中创建的文件会在名称中包含日期和时间。

CDO 最多可以将 100,000 个活动会话导出至 CSV 文件。如果来自所有设备的会话总数超过最大限制，则可以使用**按设备查看 (View By Device)** 过滤器并为各个设备生成报告。

步骤 1 在 CDO 导航窗格中，点击 **VPN > 远程访问 VPN 监控 (Remote Access VPN Monitoring)**。

步骤 2 在**按设备查看 (View By Devices)** 区域中，选择以下选项之一：

- **所有设备 (All Devices)**，可从其下面列出的所有设备导出活动会话。
- 点击要导出其会话的设备。

步骤 3 点击右上角的  图标。CDO 会将您在屏幕上看到的规则导出至 .csv 文件。

步骤 4 在电子表格应用中打开 .csv 文件，对结果进行排序和过滤。

断开 ASA 用户的活动 RA VPN 会话

您可以在 ASA 设备上终止所有用户的所有活动 RA VPN 会话。您可以在实时和历史模式下执行此任务。

CDO 会提供“VPN 会话管理器”用户角色，以允许用户查看和终止 VPN 会话。有关详细信息，请参阅用户角色。

步骤 1 在 CDO 导航窗格中，点击 **VPN** > **远程访问 VPN 监控**。

步骤 2 在**按设备查看 (View By Devices)** 区域中，点击要结束该设备上所有活动会话的 ASA 设备。

步骤 3 点击右上角显示的 Terminate All Sessions。

步骤 4 点击 Yes, Terminate All Sessions（是，终止所有会话）以确认您的选择。

断开用户的所有活动 *RA VPN* 会话

当您断开用户连接时，CDO 将终止该 ASA 设备上的所有活动 RA VPN 会话。您可以在实时和历史模式下执行此任务。

步骤 1 在 CDO 导航窗格中，点击 **VPN** > **远程访问 VPN 监控**。

步骤 2 搜索要断开其会话的用户。您可以在**搜索 (Search)** 栏中键入搜索条件。

步骤 3 点击活动会话，然后在右侧的**操作 (Actions)** 窗格中，点击**终止此用户的所有 RA VPN 会话 (Terminate all RA VPN sessions for this user)** 链接。

ASA 模板

模板使用户能够构建设备/服务配置，以便他们可以将该配置应用于已组合在一起的其他配置。这些模板提供了一个进行更改的位置，以便影响组合在一起的许多实施者。

ASA 模板参数

创建新模板时，您可能希望根据特定设备对其进行建模。CDO 提供根据模板建模所依据的设备配置中的选定文本字段设置模板参数的功能。可以从现有参数创建、设置参数，并在模板参数视图中搜索参数。

Note 如果您选择导入 ASA 模板的配置，则该配置必须采用 JSON 格式。

创建新参数

步骤 1 载入现有设备后，导航至 CDO 顶部的“模板”选项卡。

步骤 2 选择新建模板或管理模板。

步骤 3 选择所需的配置以创建参数。

步骤 4 通过在屏幕顶部的名称字段中键入来命名模板。

步骤 5 选择要向其添加参数的所需文本字段。

步骤 6 为参数提供说明、添加值和任何必要的注释。

步骤 7 点击名称 (Name) 字段旁边的保存 (Save) 以保存参数。

步骤 8 然后，您可以通过点击查看模板来查看模板。

您现在有一个已保存的参数，该参数将应用于未来使用此模板载入的所有设备。

创建新的 ASA、ISR 或 ASR 模板

基本配置

从已知的 ASA、ISR 或 ASR 基本配置开始。选择所需的配置以开始模板的参数化。参数化涉及选择配置文件中的字段或属性，并标识将在配置文件实例化时选择的值列表。

Note 如果您选择导入 ASA 模板的配置，则该配置必须采用 JSON 格式。

添加参数

选择基本配置后，即可开始参数化过程。从配置编辑器中，选择所需的参数化字段。请注意，所选字符串括在双括号中。在左侧窗格中，可以重命名参数、添加说明以及添加多个值。选择“允许自定义值”(Allow Custom Value) 可在实例化时设置自定义值。否则，只能选择已识别的值。

参数化完成后，确定模板的名称，然后点击保存。

在此处了解有关参数化的更多信息。 ASA 模板参数, on page 123

审核

保存模板后，点击审核以进入审核流程。在查看时，可以按原样导出模板，包括参数化值。请注意，这不一定是有效的配置，但提供了一种方法来查看存储在 CDO 中的模板。如果需要，也可以通过点击编辑来编辑模板。Diff 按钮可以演示保存的模板和最新编辑之间的差异。

从模板生成 ASA 配置

从模板创建配置

选择从模板配置按钮，开始从模板生成自定义配置的过程。列出可用模板，选择所选模板，然后点击选择模板。

在大多数情况下，模板将包含必须在导出时设置的参数化值，以提供自定义配置。在左侧窗格中，根据需要选择此配置的每个参数和值。请注意，这些值在编辑器中进行了演示。这些是将在导出时替换参数的值。设置所有参数值后，点击导出按钮以导出配置并下载。如果模板不包含参数化值，请点击导出按钮按原样导出配置。

管理 ASA 模板

通过管理模板视图，您可以查看所有现有模板以及对其进行编辑和删除。可以在编辑模板时修改参数化和值配置。只需将鼠标悬停在现有模板上，然后选择编辑即可进行更改。

编辑模板

进入编辑视图后：

- 通过双击或突出显示编辑器中的文本来添加参数。
- 通过在说明文本框中键入来说明参数。然后点击**添加值 (Add Value)**。
- 提供值并添加注释。点击**添加 (Add)**。
- 完成后，点击**保存**。
- 现在，您可以通过点击**查看模板 (Review Template)** 来查看模板。
  - 您可以通过点击**差异 (Diff)** 来比较文件。
  - 要导出模板，请点击**导出 (Export)**。

API 令牌

开发人员在进行 CDO REST API 调用时使用 CDO API 令牌。必须在 REST API 授权报头中插入 API 令牌，调用才能成功。API 令牌是“长期”访问令牌，不会过期；但是，您可以续订和撤销它们。

您可以从 CDO 中生成 API 令牌。这些令牌仅在生成后立即可见，并且只要“常规设置”页面处于打开状态。如果您在CDO中打开另一个页面并返回到“常规设置”页面，则该令牌不再可见，但很明显已发出令牌。

个人用户可以为特定租户创建自己的令牌。一个用户不能代表另一个用户生成令牌。令牌特定于账户-租户对，不能用于其他用户-租户组合。

API 令牌格式和声明

API 令牌是 JSON Web 令牌 (JWT)。要了解有关 JWT 令牌格式的更多信息，请阅读 JSON Web 令牌简介。https://jwt.io/introduction/

CDO API 令牌提供以下一组声明：

- id - 用户/设备 uid
- parentId - 租户 uid
- ver - 公钥的版本（初始版本为 0，例如 cdo_jwt_sig_pub_key.0）
- 订用 - 订用（可选）安全服务交换
- client_id - " api-client "

- jti - 令牌 ID

将 ASA 配置迁移到 FDM 管理 设备模板

Attention Firepower 设备管理器 (FDM) 支持和功能仅应要求提供。如果您的租户上尚未启用 防火墙设备管理器 支持，则无法管理或部署到 FDM 管理 设备。向支持团队发送请求以启用此平台。通过 TAC 打开提交支持请求

思科防御协调器 可帮助您将 ASA 迁移到 FDM 管理 设备。CDO 提供了一个向导来帮助您将 ASA 的运行配置的这些元素迁移到 FDM 管理 模板：

- 访问控制规则 (ACL)
- 接口
- 网络地址转换 (NAT) 规则
- 网络对象和网络组对象
- 路由
- 服务对象和服务组对象
- 站点间 VPN

将 ASA 运行配置的这些元素迁移到 FDM 管理 模板后，即可将 FDM 模板应用于由 CDO 管理的新 FDM 管理 设备。FDM 管理 设备采用模板中定义的配置，因此，FDM 管理 设备现在配置了 ASA 运行配置的某些方面。

使用此过程不会迁移 ASA 运行配置的其他元素。这些其他元素在 FDM 管理 设备模板中由空值表示。将模板应用于 FDM 管理 设备时，我们会应用迁移到新 FDM 管理 设备的值并忽略空值。无论新 FDM 管理 设备具有哪些其他默认值，它都会保留。我们未迁移的 ASA 运行配置的其他元素将需要在迁移过程之外在 FDM 管理 设备上重新创建。

有关使用 CDO 将 ASA 迁移到 FDM 管理 设备的过程的完整说明，请参阅使用思科防御协调器将 ASA 迁移到 FDM 托管设备。

管理 ASA 证书

数字证书为设备和个人用户的身份验证提供数字标识。数字证书包括用于识别设备或用户的信息，例如名称、序列号、公司、部门或 IP 地址。数字证书还包括用户或设备的公钥副本。有关数字证书的详细信息，请参阅思科 ASA 系列常规操作 ASDM 配置的“基本设置”一书 X.Y 文档中的“数字证书”一章。

证书颁发机构 (CA) 是指“签署”证书以确认其真实性，从而确保设备或用户的身份的可信颁发机构。CA 还颁发身份证书。

- **身份证书 (Identity Certificate)** - 内部身份证书是用于特定系统或主机的证书。您可以使用 OpenSSL 工具包自己生成这些证书，也可以从证书颁发机构获取这些证书。此外，您还可以生成自签名证书。CA 会颁发身份证书，这是特定系统或主机的证书。
- **受信任 CA 证书 (Trusted CA Certificate)** - 受信任 CA 证书是系统可用于签署其他证书的证书。这些证书与内部身份证书的区别在于基本限制条件扩展和 CA 标记方面，CA 证书启用了这些功能，而身份证书中则禁用了这些功能。受信任 CA 证书是自签名证书，也称为根证书。

远程访问 VPN 使用数字证书对安全网关和 AnyConnect 客户端（终端）进行身份验证，以建立安全的 VPN 连接。有关详细信息，请参阅远程访问 VPN 基于证书的身份验证。

证书安装指南

请阅读以下有关在 ASA 上安装证书的准则：

- 证书可以同时安装在单个或多个 ASA 设备上。
- 一次只能安装一个证书。
- 证书只能安装在实时 ASA 设备上，而不能安装在模态设备上。

ASA 证书安装

您必须将数字证书作为信任点对象上传，并将其安装在 CDO 管理的 ASA 设备上。信任点对象

注释 确保 ASA 设备没有带外更改，并且已部署所有暂存更改。

下面列出了 CDO 支持的数字证书和格式：

- 可以使用以下方法安装身份证书：
  - PKCS12 文件导入。
  - 自签名证书
  - 证书签名请求 (CSR) 导入。
- 可以使用 PEM 或 DER 格式安装受信任 CA 证书。

观看演示如何使用 CDO 在 ASA 上安装证书的截屏视频。https://www.youtube.com/watch?v=9ihOs_AmQ8s它还显示修改、导出和删除已安装证书的步骤。

支持的证书格式

- PKCS12：PKCS#12、P12 或 PFX 格式是一种二进制格式，用于在一个可加密文件中存储服务器证书、任何中间证书和私钥。PFX 文件通常具有 .pfx 和 .p12 等扩展名。

- PEM：PEM（原为“隐私增强邮件”）文件包含 ASCII（或 Base64）编码数据，证书文件可以是 .pem、.crt、.cer 或 .key 格式。它们是 Base64 编码的 ASCII 文件，包含“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”语句。
- DER：DER（可分辨编码规则）格式只是证书的二进制形式，而不是 ASCII PEM 格式。它的文件扩展名有时为 .der，但文件扩展名通常为 .cer，因此区分 DER.cer 文件和 PEM.cer 文件的唯一方法是在文本编辑器中打开该文件，然后查找 BEGIN/END 语句。与 PEM 不同，DER 编码文件不包含纯文本语句，例如 -----BEGIN CERTIFICATE-----。

信任点屏幕

将 ASA 设备载入 CDO 后，在设备和服务选项卡上，选择 ASA 设备，然后在左侧的管理窗格中点击信任点。

在“信任点”选项卡中，您将看到设备上已安装的证书。

- “已安装”状态表示已在设备上成功安装相应的证书。
- “未知”状态表示相应的证书不包含任何信息。您需要将其删除并使用正确的详细信息重新上传。CDO 发现所有未知证书都是受信任的 CA 证书。
- 点击显示“已安装”的行，在右侧窗格中查看证书详细信息。点击“更多”可查看所选证书的其他详细信息。
- 已安装的身份证书可以 PKCS12 或 PEM 格式导出，并导入到其他 ASA 设备中。请参阅“导出身份证书”。
- 只能修改已安装证书的高级设置。
  - 点击编辑以修改高级设置。
  - 进行更改后，点击发送以安装更新的证书。

使用 PKCS12 安装身份证书

您可以选择为 PKCS12 格式创建的现有信任点对象，并将其安装在 ASA 设备上。您还可以从安装向导创建新的信任点对象，并在 ASA 设备上安装证书。

开始之前

- 阅读证书安装指南。证书安装指南，第 127 页
- ASA 必须处于“已同步”状态和“在线”状态。

步骤 1 在导航栏中，点击 **设备和服务**。

步骤 2 要在单个 ASA 设备上安装身份证书，请执行以下操作：

a) 点击**设备**选项卡。

b) 点击 ASA 选项卡并选择 ASA 设备。
c) 在左侧的**管理 (Management)** 窗格中，点击**信任点 (Trustpoints)**。
d) 点击 **Install**。

注释 您还可以在多个 ASA 设备上安装证书。选择多个 ASA 设备，然后在右侧的设备操作中，点击安装证书。

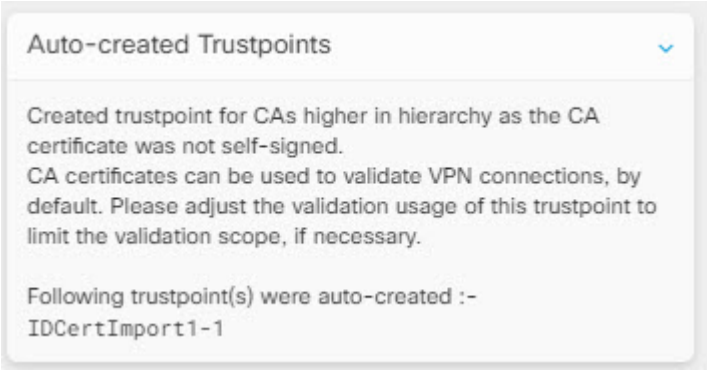
步骤 3 从选择要安装的信任点证书中，点击以下选项之一：

- 创建以添加新的信任点对象。有关更多信息，请参阅使用 PKCS12 添加身份证书对象。
- **选择**以选择 PKCS 类型的认证登记对象。

步骤 4 点击**发送 (Send)**。

这将在 ASA 设备上安装证书

注释 如果要导入已安装中间 CA 的 PKCS12 证书，ASA 会自动在设备上为尚未安装的每个中间 CA 证书创建并安装信任点对象。当您点击身份证书时，您会在右侧窗格中看到一条消息，如以下示例所示。



使用自签注册安装证书

您可以选择为自签名证书创建的现有信任点对象，并将其安装在ASA设备上。您还可以从安装向导创建新的信任点对象，并在 ASA 设备上安装证书。

开始之前

- 阅读证书安装指南。证书安装指南，第 127 页
- ASA 必须处于“已同步”状态和“在线”状态。

步骤 1 在导航栏中，点击 **设备和服务**。
步骤 2 要在单个 ASA 设备上安装身份证书，请执行以下操作：

a) 点击**设备**选项卡。
b) 点击 ASA 选项卡并选择 ASA 设备。
c) 在左侧的**管理 (Management)** 窗格中，点击**信任点 (Trustpoints)**。
d) 点击 **Install**。

注释 您还可以在多个 ASA 设备上安装签名证书。选择多个 ASA 设备，然后在右侧的设备操作中，点击安装证书。

步骤 3 从选择要安装的信任点证书中，点击以下选项之一：

- 创建以添加新的信任点对象。有关更多信息，请参阅使用 PKCS12 添加身份证书对象。
- **选择**选择自签名类型的认证登记对象。

步骤 4 点击**发送 (Send)**。

对于自签名注册类型的信任点，颁发者常用名状态将始终显示 ASA 设备，因为受管设备会充当自己的 CA，而不需要 CA 证书来生成自己的身份证书。

管理证书签名请求 (CSR)

您必须首先生成 CSR 请求，然后由受信任的证书颁发机构 (CA) 签署此请求。然后，您可以在 ASA 设备上安装由 CA 颁发的签名身份证书。

- 阅读证书安装指南。证书安装指南 ， 第 127 页
- ASA 必须处于“已同步”状态和“在线”状态。

下图描述了在 ASA 中生成 CSR 和安装已认证的证书的工作流程：

生成 CSR 请求

步骤 1 在导航栏中，点击 **设备和服务**。

步骤 2 点击**设备**选项卡。

步骤 3 点击 ASA 选项卡并选择 ASA 设备。

步骤 4 要在单个 ASA 设备上安装身份证书，请执行以下操作：

步骤 5 点击 **Install**。

步骤 6 从选择要安装的信任点证书中，点击以下选项之一：

- 创建以添加新的信任点 CSR 对象。有关详细信息，请参阅为证书签名请求 (CSR) 添加身份证书对象。
- 选择以选择已创建的 CSR 请求信任点。

步骤 7 点击**发送 (Send)**。

这会生成未签名的证书签名请求 (CSR)。

步骤 8 点击复制图标 copy_icon.png 以复制 CSR 详细信息。您还可以下载“.csr”文件格式的 CSR 请求。

步骤 9 点击**确定 (OK)**。

步骤 10 提交证书签名请求 (CSR) 到证书颁发机构，以便签署证书。

安装证书颁发机构颁发的签名身份证书

CA 颁发签名证书后，将其安装在 ASA 设备上

步骤 1 在“信任点”屏幕中，点击状态为“等待签名证书安装”的 CSR 请求，然后在右侧的“操作”窗格中，点击安装认证 ID 证书。

步骤 2 上传从 CA 收到的签名证书。您可以拖放文件或将其内容粘贴到提供的字段中。根据您选择的信任点生成信任点命令。

步骤 3 点击**发送 (Send)**。

这会将签名的身份证书安装到 ASA 设备。安装证书会立即将更改部署到设备。

注释 您还可以在多个 ASA 设备上安装证书。选择多个 ASA 设备，然后在右侧的设备操作中，点击安装证书。

在 ASA 中安装受信任 CA 证书

开始之前

- 阅读证书安装指南。证书安装指南，第 127 页

- ASA 必须处于“已同步”状态和“在线”状态。

步骤 1 在导航菜单中，点击**设备和服务 (Devices & Services)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击 ASA 选项卡并选择 ASA 设备。

步骤 4 要在单个 ASA 设备上安装身份证书，请执行以下操作：

a) 选择 ASA 设备，然后在右侧的**管理 (Managemento** 窗格中，点击**信任点 (Trustpoints)**。

b) 点击 **Install**。

注释 您还可以在多个 ASA 设备上安装证书。选择多个 ASA 设备，然后在右侧的设备操作中，点击安装证书。

步骤 5 从选择要安装的信任点证书中，点击以下选项之一：

- 创建以添加新的信任点对象。有关详细信息，请参阅添加受信任 CA 证书对象。
- **选择**选择一个受信任证书颁发机构对象。

步骤 6 点击**发送 (Send)**。

这会在 ASA 设备上安装受信任的 CA 文件。

导出身份证书

您可以 PKCS12 或 PEM 格式导出和导入密钥对，以及与某个信任点关联的已颁发证书。此格式对于在其他 ASA 上手动复制信任点配置来说非常有用。

SUMMARY STEPS

1. 在导航菜单中，点击**设备和服务 (Devices & Services)**。
2. 点击**设备**选项卡。
3. 点击 **ASA**。
4. 选择 ASA 设备，然后在右侧的 **Management** 中点击 **Trustpoints**。
5. 点击身份证书以导出证书配置。或者，您可以通过在搜索字段中输入证书名称来搜索证书。
6. 在右侧的**操作**窗格中，点击**导出证书**。
7. 通过点击 **PKCS12 格式 (PKCS12 Format)** 或 **PEM 格式 (PEM Format)** 来选择证书格式。
8. 输入用于加密要导出的 PKCS12 文件的加密密码。
9. 确认加密密码。
10. 点击**导出 (Export)** 以导出证书配置。

DETAILED STEPS

	命令或操作	目的
步骤 1	在导航菜单中，点击**设备和服务 (Devices & Services)**。	
步骤 2	点击**设备**选项卡。	
步骤 3	点击 **ASA**。	
步骤 4	选择 ASA 设备，然后在右侧的 **Management** 中点击 **Trustpoints**。	
步骤 5	点击身份证书以导出证书配置。或者，您可以通过在搜索字段中输入证书名称来搜索证书。	
步骤 6	在右侧的**操作**窗格中，点击**导出证书**。	
步骤 7	通过点击 **PKCS12 格式 (PKCS12 Format)** 或 **PEM 格式 (PEM Format)** 来选择证书格式。	
步骤 8	输入用于加密要导出的 PKCS12 文件的加密密码。	
步骤 9	确认加密密码。	
步骤 10	点击**导出 (Export)** 以导出证书配置。	系统将显示一个信息对话框，通知您证书配置文件已成功导出到指定的位置。

编辑已安装的证书

您只能修改已安装证书的高级选项。

步骤 1 在导航菜单中，点击**设备和服务 (Devices & Services)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击 **ASA** 选项卡。

步骤 4 选择 ASA 设备，然后在右侧的 **Management** 中点击 **Trustpoints**。

步骤 5 点击要修改的证书，然后在右侧的**操作**窗格中，点击**编辑**。

步骤 6 修改所需的参数并点击**保存**。

从 ASA 删除现有证书

您可以逐个删除证书。在删除证书后，无法将其恢复。

步骤 1 在导航菜单中，点击**设备和服务 (Devices & Services)**。

步骤 2 选择 ASA 设备，然后在右侧的“管理”中，点击“信任点”。

步骤 3 点击要删除的证书，然后在右侧的操作窗格中，点击删除。

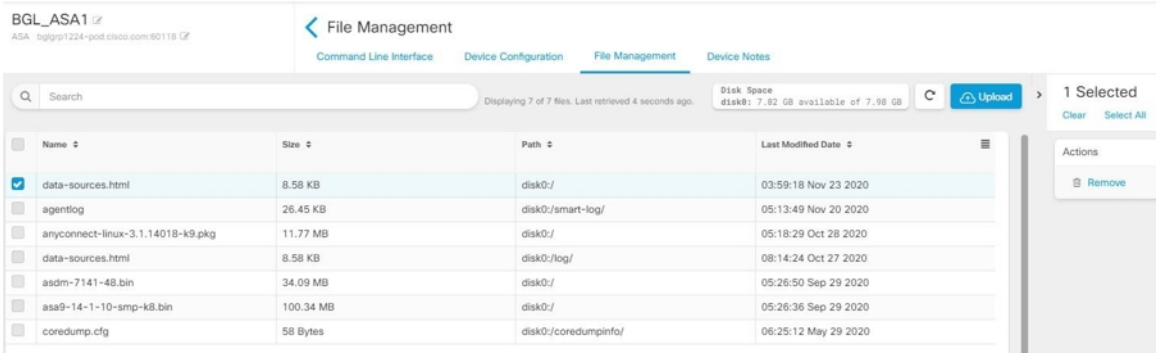
步骤 4 点击确定以删除所选证书。

ASA 文件管理

CDO 提供文件管理工具来帮助您执行基本的文件管理任务，例如查看、上传或删除 ASA 设备的闪存 (disk0) 空间中的文件。

Note 您无法管理 disk1 上的文件。

File Management 屏幕列出了设备闪存（disk0）上的所有文件。成功上传文件后，您可以点击刷新图标查看文件。默认情况下，此屏幕每 10 分钟自动刷新一次。磁盘空间字段显示 disk0 目录上的磁盘空间量。



您可以将 AnyConnect 映像上传到单个或多个 ASA 设备。成功上传后，AnyConnect 映像将与所选 ASA 设备上的 RA VPN 配置相关联。这有助于您将新发布的 AnyConnect 软件包同时上传到多个 ASA 设备。

将文件上传到闪存系统

CDO 仅支持从远程服务器上传基于 URL 的文件。支持的文件上传协议包括 HTTP、HTTPS、TFTP、FTP、SMB 或 SCP。您可以将任何文件（例如 AnyConnect 软件映像、DAP.xml、data.xml）和主机扫描映像文件上传到单个或多个 ASA 设备。

Note 如果远程服务器的 URL 路径无效或可能出现任何问题，CDO 不会将文件上传到选定的 ASA 设备。您可以导航至设备工作流程以了解更多详细信息。

假设设备配置为高可用性，CDO 首先将文件上传到备用设备，并且只有在成功上传后，才会将文件上传到主用设备。在文件删除过程中应用相同的行为。

用于上传文件的受支持协议的语法：

协议	语法	示例
HTTP	http://[[path/]filename]	http://www.geonames.org/data-sources.html
HTTPS	https://[[path/]filename]	https://docs.aws.amazon.com/amazov/tagging.html
TFTP	tftp://[[path/]filename]	tftp://10.10.16.6/ftd/components.html
FTP	ftp://[[user[:password]@]server[:port]/[path/]filename]	ftp://[redacted]
中小企业	smb://[[path/]filename]	smb://10.10.32.145//sambashare/hello.txt
SCP	scp://[[user[:password]@]server[/path]/filename]	scp://rootciscol23@10.10.16.6//root/events_send.py

准备工作

- 确保可从 ASA 设备访问远程服务器。
- 确保文件已上传到远程服务器。
- 确保存在从 ASA 设备到该服务器的网络路由。
- 如果在 URL 中使用 FQDN，请确保已配置 DNS。
- 远程服务器的 URL 必须是不提示进行身份验证的直接链接。
- 如果远程服务器 IP 地址经过 NAT，则必须提供远程服务器位置的 NAT 公共 IP 地址。

Note 如果将文件上传到在故障切换中配置为对等体的 ASA，则 CDO 不会为故障切换对中的另一个对等体确认新文件，并且设备状态更改为“未同步”。您必须手动将更改部署到两台设备，以便 CDO 识别两台设备中的文件。

将文件上传到单个 ASA 设备

使用此程序将文件上传到单个 ASA 设备。

步骤 1 在导航栏中，点击 **设备和服务**。

步骤 2 点击**设备**选项卡。

步骤 3 点击 ASA 选项卡并选择 ASA 设备。

步骤 4 在右侧的**管理 (Management)** 窗格中点击**文件管理 (File Management)**。您可以查看 ASA 设备上的可用磁盘空间和文件。

步骤 5 点击右边的**上传 (Upload)** 按钮。

步骤 6 在 **URL 链接**中，指定预上传文件的服务器路径。**Destination Path** 字段显示正在上传到 **disk0** 目录的文件的名称。如果要将文件上传到 disk0 中的特定目录，请在此字段中指定其名称。例如，如果要将 dap.xml 文件上传到“DAPFiles”目录，请在字段中指定“**disk0:**/DAPFiles/dap.xml”。

Note 您可以通过在 CDO ASA CLI 接口中执行 **dir** 命令来查看 disk0 文件夹中的目录。

步骤 7 如果指定的服务器路径指向 AnyConnect 文件，则**将文件与 RA VPN 配置关联**复选框处于启用状态。 注意：仅对遵循正确命名约定的 AnyConnect 文件名（即“anyconnect-win-xxx.pkg”、“anyconnect-linux-xxx.pkg”或“anyconnect-mac-xxx”）启用此复选框。 pkg' 格式。选中此复选框后，CDO 会在成功上传后将 AnyConnect 文件关联到所选 ASA 设备上的 RA VPN 配置。

步骤 8 点击**上传**。CDO 将文件上传到设备。

步骤 9 如果您已在步骤 5 中选择将 AnyConnect 软件包与 RA VPN 配置相关联，请将配置更改从 CDO 部署到 ASA。

What to do next

您不必在设备上部署配置更改。

将文件上传到多个 ASA 设备

使用此程序将文件同时上传到多个 ASA 设备。

步骤 1 在导航栏中，点击 **设备和服务**。

步骤 2 点击**设备**选项卡。

步骤 3 点击 **ASA** 选项卡并选择多个 ASA 设备以执行批量上传。

步骤 4 在右侧的**设备操作 (Device Actions)** 窗格中，点击**上传文件 (Upload File)**。注意：如果 ASA 设备在线，系统将显示**上传文件**链接。

步骤 5 在 **URL 链接**中，指定预上传文件的服务器路径。**Destination Path** 字段显示正在上传到 **disk0** 目录的文件的名称。如果要将文件上传到 disk0 中的特定目录，请在此字段中指定其名称。例如，如果要将 dap.xml 文件上传到“DAPFiles”目录，请在字段中指定“**disk0:**/DAPFiles/dap.xml”。

Note 您可以通过在 CDO ASA CLI 接口中执行 **dir** 命令来查看 disk0 文件夹中的目录。

步骤 6 如果指定的服务器路径指向 AnyConnect 文件，则**将文件与 RA VPN 配置关联**复选框处于启用状态。

Note 仅对遵循正确命名约定的 AnyConnect 文件名（即“anyconnect-win-xxx.pkg”、“anyconnect-linux-xxx.pkg”或“anyconnect-mac-xxx.pkg”）启用此复选框。格式。选中此复选框后，CDO 会在成功上传后将 AnyConnect 文件关联到所选 ASA 设备上的 RA VPN 配置。

步骤 7 点击**上传**。

步骤 8 如果您已在步骤 4 中选择将 AnyConnect 软件包与 RA VPN 配置关联，请将配置更改从 CDO 部署到 ASA。

What to do next

您可以查看在各个设备上上传文件的进度。选择 ASA 设备，然后在右侧的**管理 (Management)** 窗格中点击**文件管理 (File Management)**。如果文件上传正在进行，请等待操作完成。

您不必在设备上部署配置更改。

从 ASA 中删除文件

不允许删除与 RA VPN 配置关联的 AnyConnect 文件。您必须取消 AnyConnect 文件与相应的 RA VPN 配置的关联，然后从文件管理工具中删除该文件。

Note 如果将文件上传到在故障切换中配置为对等体的 ASA，则 CDO 不会为故障切换对中的另一个对等体确认新文件，并且设备状态更改为**未同步**。您必须手动将更改部署到**两台**设备，以便 CDO 识别两台设备中的文件。

删除操作会从闪存中永久删除所选文件。删除文件时，系统会显示一条消息，要求确认。使用以下程序从所选 ASA 设备中删除文件：

步骤 1 在导航栏中，点击 **设备和服务**。

步骤 2 点击**设备**选项卡。

步骤 3 点击 **ASA** 选项卡并选择 ASA 设备。

步骤 4 在右侧的**管理 (Management)** 窗格中点击**文件管理 (File Management)**。

步骤 5 选择要删除的文件，然后在右侧的**操作**下，点击**删除**。最多可以选择 25 个文件。如果 CDO 无法删除某些文件，您可以查看设备**工作流程**以确定已删除和保留的文件。

步骤 6 如果您已选择删除 AnyConnect 软件包，请将配置更改从 CDO 部署到 ASA。

管理 ASA 高可用性

在主用-主用故障切换模式下对 ASA 所做的配置更改

当 Cisco Defense Orchestrator (CDO) 使用 CDO 上的暂存配置更改 ASA 的运行配置时，或者当它使用 ASA 上存储的配置更改 CDO 上的配置时，它会尝试仅更改配置文件的相关行（如果该方面存在）的配置可以通过 CDO GUI 进行管理。如果无法使用 CDO GUI 进行所需的配置更改，CDO 会尝试覆盖整个配置文件以进行更改。

以下是两个示例：

- 您可以使用 CDO GUI 创建或更改网络对象。如果 CDO 需要将该更改部署到 ASA 的配置中，则会在发生更改时覆盖 ASA 上正在运行的配置文件的相关行。
- 您无法使用 CDO GUI 创建新的 ASA 用户。如果使用 ASA 的 ASDM 或 CLI 将新用户添加到 ASA，当该带外更改被接受且 CDO 更新存储的配置文件时，CDO 会尝试覆盖在 CDO 上暂存的 ASA 的整个配置文件。

在主用-主用故障切换模式下配置 ASA 时，不遵循这些规则。当 CDO 管理在主用-主用故障切换模式下配置的 ASA 时，CDO 无法始终将所有配置更改从自身部署到 ASA 或将所有配置更改从 ASA 读取到自身中。以下是这种情况的两种情况：

- 在 CDO 中对 ASA 的配置文件所做的更改（CDO 在 CDO GUI 中不支持）无法部署到 ASA。此外，对 CDO 不支持的配置文件所做的更改，以及对 CDO 支持的配置文件所做的更改，都无法部署到ASA。在这两种情况下，您都会收到错误消息：“CDO 目前不支持在故障切换模式下替换设备的完整配置。请点击“取消”并手动将更改应用到设备。”与CDO界面中的消息一起，您会看到已禁用的替换配置按钮。
- CDO 不会拒绝对在主用-主用故障切换模式下配置的ASA所做的带外更改。如果对ASA的运行配置进行带外更改，则 ASA 会在“设备和服务”(Devices & Services) 页面上标记为“检测到冲突”(Conflict Detected)。如果您查看冲突并尝试拒绝，CDO 会阻止该操作。您收到消息“CDO 不支持拒绝此设备的带外更改。此设备正在运行不受支持的软件版本，或者是主用/主用故障切换对的成员。请点击“继续”以接受带外更改。”

⚠

Caution 如果您发现自己必须接受来自 ASA 的带外更改，则在 CDO 上暂存但尚未部署到 ASA 的任何配置更改都将被覆盖并丢失。

当 CDO GUI 支持这些更改时，CDO 支持在故障切换模式下对 ASA 进行的配置更改。

相关信息：

在 ASA 上配置 DNS

使用此程序在每个 ASA 上配置域名服务器 (DNS)。

前提条件

- ASA 必须能够访问互联网。
- 在开始安装之前收集这些信息：
  - 可以访问 DNS 服务器的 ASA 接口的名称；例如，inside、outside 或 dmz。
  - 您的组织使用的 DNS 服务器的 IP 地址。如果您不维护自己的 DNS 服务器，可以使用思科 Umbrella。思科 Umbrella 的 IP 地址为 208.67.220.220。

操作步骤

步骤 1 在导航栏中，点击**设备和服务 (Devices & Services)**。

步骤 2 点击**设备 (Devices)** 选项卡。

步骤 3 点击 **ASA** 选项卡，然后选择要配置 DNS 的所有 ASA。

步骤 4 在右侧的操作窗格中，选择**命令行接口 (Command Line Interface)**。

步骤 5 点击 CLI 宏收藏夹星标。

步骤 6 在宏面板中选择配置 DNS 宏。

步骤 7 选择 > 视图参数，然后在参数列中填写以下参数的值：

- IF_Name - 可以访问 DNS 服务器的 ASA 接口的名称。
- IP_ADDR - 您的组织使用的 DNS 服务器的 IP 地址。

步骤 8 点击**发送到设备 (Send to devices)**。

CDO 命令行界面

CDO 为用户提供命令行界面 (CLI)，用于管理 ASA 设备。用户可以将命令发送到单个设备或同时发送到多个设备。

相关信息：

- 有关详细的 ASA CLI 文档，请参阅ASA 命令行接口文档。

使用命令行接口

步骤 1 打开**清单 (Inventory)** 页面。

步骤 2 点击“清单”(Inventory) 表上方的**设备 (Devices)** 按钮。

步骤 3 使用设备选项卡和过滤器按钮查找要使用命令行界面 (CLI) 管理的设备。

步骤 4 选择设备。

步骤 5 在**设备操作 (Device Actions)** 窗格中，点击**命令行接口 (Command Line Interface)**。

步骤 6 点击 **命令行接口 (Command Line Interface)**。

步骤 7 在命令窗格中输入一个或多个命令，然后点击发送。 设备对命令的响应显示在下面的“响应窗格”中。

Note 如果可以运行的命令有限制，则会在命令窗格上方列出这些限制。

Related Topics

在命令行接口中输入命令

在命令行接口中输入命令

可以在一行中输入单个命令，也可以在多行中依次输入多个命令，CDO 将按顺序执行这些命令。以下示例发送创建三个网络对象和包含这些网络对象的网络对象组的一批命令。ASA

输入设备命令：CDO 在 的全局配置模式下执行命令。ASAASA

长命令：如果您输入一个很长的命令，CDO 会尝试将您的命令拆分为多个命令，以便可以针对 API 运行所有这些命令。如果CDO无法确定命令的正确分隔，它会提示您提示中断命令列表的位置。例如：

错误：CDO 尝试执行此命令中长度超过 600 个字符的部分。您可以通过在命令列表之间添加一个空行来向 CDO 提示适当的命令分隔点。

如果收到此错误：

步骤 1 点击 CLI 历史记录窗格中导致错误的命令。CDO 使用一长串命令填充命令框。

步骤 2 通过在相关命令组后面输入空行来编辑长命令列表。例如，在定义网络对象列表并将其添加到上述示例中的组后，添加一个空行。您可能希望在命令列表中的几个不同位置执行此操作。

步骤 3 点击**发送 (Send)**。

使用命令历史记录

发送 CLI 命令后，CDO 会在“命令行界面”(Command Line Interface) 页面的历史记录窗格中记录该命令。您可以重新运行历史记录窗格中保存的命令，或将这些命令用作模板：

步骤 1 在**清单 (Inventory)** 页面上，选择要配置的设备。

步骤 2 点击**设备 (Devices)** 选项卡以找到设备。

步骤 3 点击设备类型选项卡。

步骤 4 点击 **>_命令行接口 (>_Command Line Interface)**。

步骤 5 点击时钟图标可展开历史记录窗格（如果尚未展开）。

步骤 6 在历史记录窗格中选择要修改或重新发送的命令。

步骤 7 按原样重新使用命令，或在命令窗格中对其进行编辑，然后点击发送。CDO 在响应窗格中显示命令的结果。

Note CDO 显示 Done!两种情况下响应窗格中的消息：

- 成功执行命令后。
- 当命令没有要返回的结果时。例如，您可以发出带有正则表达式的 show 命令，用于搜索配置条目。如果没有符合正则表达式条件的配置条目，CDO 将返回 Done!。

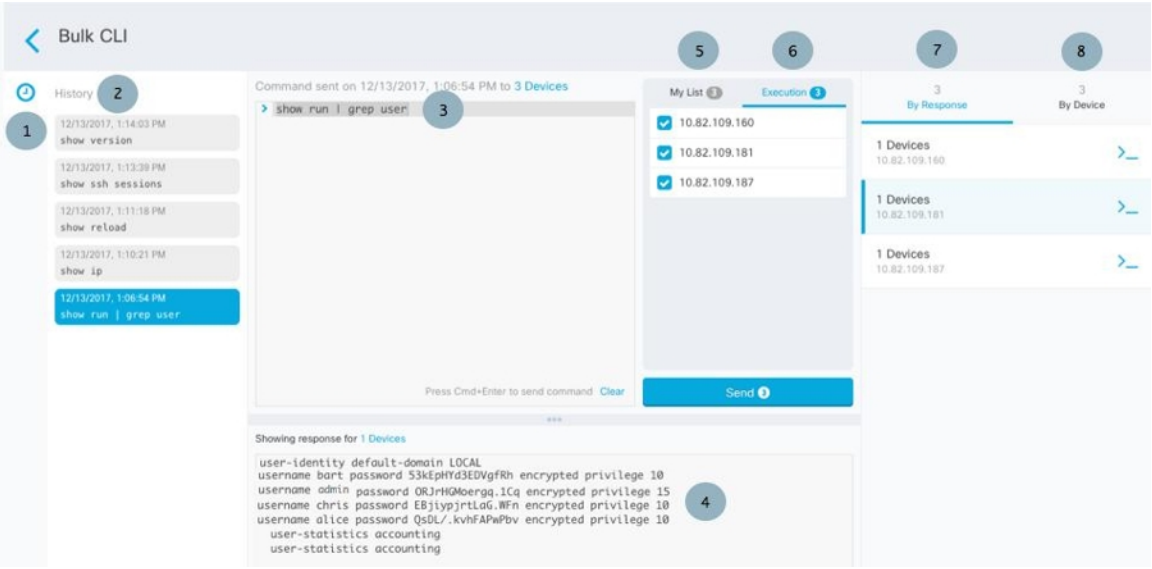
批量命令行接口

CDO 为用户提供使用命令行接口 (CLI) 管理 Secure Firewall ASA、FDM 管理 威胁防御、SSH 和 Cisco IOS 设备。用户可以将命令发送到单个设备或同时发送到多个同类设备。本节介绍一次向多台设备发送 CLI 命令。

相关信息：

- 有关详细的 ASA CLI 文档，请参阅ASA 命令行接口文档。

批量 CLI 接口



Note CDO 显示 Done!两种情况下的消息：

- 成功执行命令且无错误后。
- 当命令没有要返回的结果时。例如，您可以发出带有正则表达式的show命令，用于搜索某个配置条目。如果没有符合正则表达式条件的配置条目，CDO 将返回 Done!。

编号	说明
1	点击时钟可展开或折叠命令历史记录窗格。
2	命令历史记录。发送命令后，CDO 会在此历史记录窗格中记录该命令，以便您可以返回到该窗格，选择并再次运行该命令。
3	命令窗格。在此窗格的提示符后输入命令。
4	响应窗格。CDO 显示设备对命令的响应以及 CDO 消息。如果多个设备的响应相同，则响应窗格会显示消息“显示 X 台设备的响应”(Showing Responses for X devices)。点击 X 设备，CDO 将显示对命令返回相同响应的所有设备。 **Note** CDO 显示 Done!两种情况下的消息： • 成功执行命令且无错误后。 • 当命令没有要返回的结果时。例如，您可以发出带有正则表达式的 show 命令，用于搜索某个配置条目。如果没有符合正则表达式条件的配置条目，CDO 将返回 Done!。
5	**我的列表 (My List)** 选项卡显示您从**清单 (Inventory)** 表中选择的设备，并允许您包含或排除要向其发送命令的设备。
6	上图中突出显示的“执行”选项卡显示在历史记录窗格中选择的命令中的设备。在本例中，show run |在历史记录窗格中选择了 grep 用户命令，执行选项卡显示它已发送到 10.82.109.160、10.82.109.181 和 10.82.10.9.187。
7	点击“By Response”（按响应）选项卡将显示命令生成的响应列表。相同的响应组合在一行中。当您在“按响应”选项卡中选择一行时，CDO 会在响应窗格中显示对该命令的响应。
8	点击“按设备”选项卡会显示每个设备的单独响应。点击列表中的其中一个设备，即可查看特定设备对命令的响应。

批量发送命令

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以找到设备。

步骤 3 选择相应的设备选项卡，然后使用过滤器按钮查找要使用命令行界面配置的设备。

步骤 4 选择设备。

步骤 5 在**设备操作 (Device Actions)** 窗格中，点击**>_命令行接口 (>_Command Line Interface)**。

步骤 6 您可以在“我的列表”字段中选中或取消选中要向其发送命令的设备。

步骤 7 在命令窗格中输入命令，然后点击发送。命令输出显示在响应窗格中，命令记录在更改日志中，命令CDO在批量 CLI 窗口的历史记录窗格中记录您的命令。

Note 命令将在已同步的选定ASA设备上成功执行，但在未同步的设备上可能会失败。如果任何选定的ASA设备未同步，则仅允许使用以下命令：show、ping、traceroute、vpn-sessiondb、changeto、dir、write 和 copy。

使用批量命令历史记录

发送批量 CLI 命令后，CDO 会在“批量 CLI”页面历史记录页面中记录该命令。批量 CLI 接口您可以重新运行历史记录窗格中保存的命令，也可以将这些命令用作模板。历史记录窗格中的命令与运行这些命令的原始设备相关联。

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击 **设备** 选项卡以找到设备。

步骤 3 点击相应的设备类型选项卡，然后点击过滤器图标以查找要配置的设备。

步骤 4 选择设备。

步骤 5 点击 **命令行接口 (Command Line Interface)**。

步骤 6 在“历史记录”窗格中选择要修改或重新发送的命令。请注意，您选择的命令与特定设备相关联，而不一定是您在第一步中选择的设备。

步骤 7 查看我的列表选项卡，确保您要发送的命令将发送到您期望的设备。

步骤 8 在命令窗格中编辑命令，然后点击**发送 (Send)**。CDO 在响应窗格中显示命令的结果。

Note 命令将在已同步的选定ASA设备上成功执行，但在未同步的设备上可能会失败。如果任何选定的ASA设备未同步，则仅允许使用以下命令：show、ping、traceroute、vpn-sessiondb、changeto、dir、write 和 copy。

使用批量命令过滤器

运行批量 CLI 命令后，您可以使用“按响应”过滤器和“按设备”过滤器继续配置设备。

按响应过滤器

运行批量命令后，CDO会使用发送该命令的设备返回的响应列表填充“按响应”选项卡。具有相同响应的设备会合并到一行中。点击“按响应”(By Response) 选项卡中的行会在响应窗格中显示设备的响应。如果响应窗格显示多个设备的响应，则会显示消息“显示 X 台设备的响应”。点击 X 设备，CDO 将显示对命令返回相同响应的所有设备。

要将命令发送到与命令响应关联的设备列表，请执行以下程序：

步骤 1 点击 By Response 选项卡中一行中的命令符号。

步骤 2 查看命令窗格中的命令，然后点击发送以重新发送命令，或点击清除以清除命令窗格并输入要发送到设备的新命令，然后点击发送。

步骤 3 查看从命令收到的响应。

步骤 4 如果您确信所选设备上的运行配置文件反映了您的更改，请在命令窗格中键入 write memory，然后点击 Send。这样会将运行配置保存至启动配置。

按设备过滤器

运行批量命令后，CDO 会使用已发送命令的设备列表填充“执行”选项卡和“按设备”选项卡。点击“按设备”(By Device) 选项卡中的行会显示每个设备的响应。

要在同一设备列表上运行命令，请执行以下程序：

步骤 1 点击**按设备 (By Device)** 选项卡。

步骤 2 点击 **>_在这些设备上执行命令**。

步骤 3 点击**清除 (Clear)** 以清除命令窗格并输入新命令。

步骤 4 在我的列表窗格中，通过选中或取消选中列表中的单个设备来指定要向其发送命令的设备列表。

步骤 5 点击**发送 (Send)**。命令的响应会显示在响应窗格中。如果响应窗格显示多个设备的响应，则会显示消息“显示 X 台设备的响应”。点击 X 设备，CDO 将显示对命令返回相同响应的所有设备。

步骤 6 如果您确信所选设备上的运行配置文件反映了您的更改，请在命令窗格中键入 `write memory`，然后点击**发送 (Send)**。

命令行界面宏

CLI 宏是可以使用的完整形式的 CLI 命令，或者是可以在运行之前修改的 CLI 命令的模板。所有宏都可以在一个或多个 ASA 设备上同时运行。

使用类似模板的 CLI 宏可同时在多台设备上运行相同的命令。CLI 宏可促进设备配置和管理的一致性。使用完全格式的 CLI 宏获取有关设备的信息。您可以立即在 ASA 设备上使用不同的 CLI 宏。

您可以创建 CLI 宏来监控您经常执行的任务。有关详细信息，请参阅创建 CLI 宏。

CLI 宏是系统定义的或用户定义的。系统定义的宏由 CDO 提供，无法编辑或删除。用户定义的宏由您创建，可以编辑或删除。

Note 只有在设备载入 CDO 后，才能为设备创建宏。

以 ASA 为例，如果要查找其中一个 ASA 上的特定用户，可以运行以下命令：

```
show running-config | grep username
```

运行命令时，您要将 *username* 替换为要搜索的用户的用户名。要使用此命令来创建宏，请使用相同的命令并在用户名周围加上大括号。

```
> show running-config | grep {{username}}
```

您可以随意命名参数。您还可以使用此参数名称创建相同的宏：

```
> show running-config | grep {{username_of_local_user_stored_on_asa}}
```

参数名称可以是描述性的，并且必须使用字母数字字符和下划线。命令语法，在本例中为

```
show running-config | grep
```

命令的一部分，必须对要向其发送命令的设备使用正确的 CLI 语法。

从新命令创建 CLI 宏

步骤 1 在创建 CLI 宏之前，请在 CDO 的命令行界面中测试命令，以便确保命令语法正确并返回可靠的结果。

Note
- 有关详细的 ASA CLI 文档，请参阅ASA 命令行接口文档。

步骤 2 在导航栏中，点击**清单 (Inventory)**。

步骤 3 点击 **设备 (Devices)**选项卡以找到设备。

步骤 4 点击相应的设备类型选项卡，然后选择在线和同步的设备。

步骤 5 点击 **>_Command Line Interface**。

步骤 6 点击 CLI 宏收藏夹星标 ★，以查看已经存在的宏。

步骤 7 点击加号按钮 +。

步骤 8 请为宏指定唯一的名称。如果需要，请为 CLI 宏提供说明和注释。

步骤 9 在**命令 (Command)** 字段中输入完整命令。

步骤 10 运行命令时，将要修改的命令部分替换为用大括号括起来的参数名称。

步骤 11 点击**创建**。您创建的宏可用于该类型的所有设备，而不只是您最初指定的设备。

要运行命令，请参阅在设备上运行 CLI 宏。

从 CLI 历史记录或现有 CLI 宏创建 CLI 宏

在此程序中，您将从已运行的命令、另一个用户定义的宏或从系统定义的宏创建用户定义的宏。

步骤 1 在导航栏中，点击 **设备和服务**。

注释 如果要从CLI历史记录创建用户定义的宏，请选择运行命令的设备。CLI宏在同一账户上的设备之间共享，但不是 CLI 历史记录。

步骤 2 点击**设备**选项卡。

步骤 3 点击相应的设备类型选项卡，然后选择在线和同步的设备。

步骤 4 点击 **>_命令行接口**。

步骤 5 查找要生成 CLI 宏的命令，然后选择该命令。使用以下方法之一：

- 点击时钟 可查看您在该设备上运行的命令。选择要转换为宏的命令，命令将显示在命令窗格中。
- 点击 CLI 宏收藏夹星标 ，以查看已经存在的宏。选择要更改的用户定义或系统定义的 CLI 宏。命令显示在命令窗格中。

步骤 6 使用 命令窗格中的 命令，点击 CLI 宏金色星标 。命令现在是新 CLI 宏的基础。

步骤 7 请为宏指定唯一的名称。如果需要，请为 CLI 宏提供说明和注释。

步骤 8 查看命令字段中的命令，并进行所需的更改。

步骤 9 运行命令时，将要修改的命令部分替换为用大括号括起来的参数名称。

步骤 10 点击**创建**。您创建的宏可用于该类型的所有设备，而不只是您最初指定的设备。

要运行命令，请参阅运行 CLI 宏。

运行 CLI 宏

步骤 1 在导航栏中，点击 **设备和服务**。

步骤 2 点击**设备**选项卡。

步骤 3 点击相应的设备类型选项卡，然后选择一个或多个设备。

步骤 4 点击 **>_命令行接口**。

步骤 5 在命令面板中，点击星号 。

步骤 6 从命令面板中选择 CLI 宏。

步骤 7 使用以下两种方式之一运行宏：

- 如果宏没有要定义的参数，请点击**发送 (Send)**。命令的响应显示在响应窗格中。就行了。
- 如果宏包含参数，例如下面的配置 DNS 宏，请点击 **>_ 查看参数**。

步骤 8 在“参数”(Parameters) 窗格中，在“参数”(Parameters) 字段中填写参数的值。

步骤 9 点击 **Send**。在 CDO 成功发送命令并更新设备配置后，您会收到消息完成！

- 对于 ASA，将更新当前配置文件：

步骤 10 发送命令后，您可能会看到消息“某些命令可能已对运行配置进行了更改”(Some commands may have made changes to the running config) 以及两个链接。

- 点击**写入磁盘 (Write to Disk)** 会将此命令所做的更改以及运行配置中的任何其他更改保存到设备的启动配置中。
- 点击**消除 (Dismiss)**，可关闭消息。

编辑 CLI 宏

您可以编辑用户定义的 CLI 宏，但不能编辑系统定义的宏。编辑 CLI 宏会更改所有 ASA 设备。宏并非特定于特定设备。

步骤 1 在导航栏中，点击 **设备和服务**。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。
步骤 4 请选择您的设备。
步骤 5 点击 **命令行接口 (Command Line Interface)**。
步骤 6 选择要编辑的用户定义的宏。
步骤 7 点击宏标签中的编辑图标。
步骤 8 在编辑宏对话框中编辑 CLI 宏。
步骤 9 点击**保存 (Save)**。

有关如何运行 CLI 宏的说明，请参阅运行 CLI 宏。

删除 CLI 宏

您可以删除用户定义的 CLI 宏，但不能删除系统定义的宏。删除 CLI 宏会删除所有设备的宏。宏并非特定于特定设备。

步骤 1 在导航栏中，点击 **设备和服务**。
步骤 2 点击**设备**选项卡。
步骤 3 点击适当的设备类型选项卡。
步骤 4 请选择您的设备。
步骤 5 点击 >_**命令行接口 (Command Line Interface)**。
步骤 6 选择要删除的用户定义的 CLI 宏。
步骤 7 点击 CLI 宏标签中的垃圾桶图标 。
步骤 8 确认要删除 CLI 宏。

使用 CDO CLI 配置 ASA

您可以通过在 CDO 中提供的 CLI 界面中运行 CLI 命令来配置 ASA 设备。要使用该接口，请在**清单 (Inventory)** 菜单上选择设备，然后点击**命令行界面 (Command Line Interface)**。有关更多信息，请参阅使用 CDO 命令行接口。

添加新的日志记录服务器

系统日志记录是将来自设备的消息收集到运行系统日志后台守护程序的服务器的方法。将信息记录到中央系统日志服务器有助于汇聚日志和提醒。

有关详细信息，请参阅您正在运行的 ASA 版本的《CLI 手册 1：思科 ASA 系列常规操作 CLI 配置指南》中“日志记录”一章的“监控”部分。

配置 DNS 服务器

需要配置 DNS 服务器，以便 ASA 能够将主机名解析为 IP 地址。还必须配置 DNS 服务器，以在访问规则中使用完全限定域名 (FQDN) 网络对象。

有关详细信息，请参阅所运行 ASA 版本的《CLI 手册 1：思科 ASA 系列常规操作 CLI 配置指南》中“配置 DNS 服务器”部分的“基本设置”一章。

添加静态路由和默认路由

要将流量路由到非连接的主机或网络，必须使用静态路由或动态路由定义到主机或网络的路由。

有关详细信息，请参阅《CLI 手册 1：思科 ASA 系列常规操作 CLI 配置指南》中的“静态和默认路由”一章。

配置接口

您可以使用 CLI 命令配置管理和数据接口。有关详细信息，请参阅《CLI 手册 1：思科 ASA 系列常规操作 CLI 配置指南》的“基本接口配置”一章。

使用 CDO 来比较 ASA 配置

使用此程序可比较两个 ASA 的配置。

步骤 1 在导航菜单中，点击**清单 (Inventory)**。
步骤 2 点击**设备 (Devices)** 选项卡以查找 ASA 设备，或点击**模板 (Templates)** 选项卡以查找 ASA 型号设备。
步骤 3 点击 **ASA** 选项卡。
步骤 4 过滤要比较的设备的设备列表。
步骤 5 选择两个 ASA。它们的状态无关紧要。您正在比较 Defense Orchestrator 上存储的 ASA 配置。
步骤 6 在右侧的“设备操作”(Device Actions) 窗格中，点击 **比较 (Compare)**。
步骤 7 在比较配置对话框中，点击**下一步**和**上一步**可跳过配置文件中以蓝色突出显示的差异。

ASA 批量 CLI 使用案例

以下情况是您对 ASA 设备使用 CDO 的批量 CLI 功能时可能遇到的工作流程。

显示 ASA 的运行配置中的所有用户，然后删除其中一个用户

步骤 1 在导航栏中，点击 **设备和服务**。
步骤 2 点击**设备 (Devices)** 选项卡以找到设备。

步骤 3 点击 **ASA** 选项卡。

步骤 4 搜索并过滤要从中删除用户的设备的设备列表，然后选择这些设备。

Note 确保您选择的设备已同步。设备未同步时，仅允许使用以下命令：show、ping、traceroute、vpn-sessiondb、changeto、dir、copy 和 write。

步骤 5 在详细信息窗格中点击 **>_命令行接口 (>_Command Line Interface)**。CDO 列出您在我的列表窗格中选择的设备。如果您决定将命令发送到更少的设备，请取消选中该列表中的设备。

步骤 6 在命令窗格中，输入 show run | grep user，然后点击 Send。 运行配置文件中包含字符串 user 的所有行都将显示在响应窗格中。系统将打开“执行”选项卡，显示执行命令的设备。

步骤 7 点击按响应选项卡并查看响应，以确定哪些设备具有要删除的用户。

步骤 8 点击我的列表选项卡，然后选择要从中删除用户的设备列表。

步骤 9 在命令窗格中，输入 no 形式的 user 命令以删除 user2，然后点击 Send。在本示例中，您将删除 user2：
no user user2 password reallyhardpassword privilege 10

步骤 10 在历史记录面板中查找 show run | 的实例。用于搜索用户名的 grep user 命令。选择该命令，查看“执行”列表中的设备列表，然后选择“发送”。您应该会看到用户名已从您指定的设备中删除。

步骤 11 如果您确信已从运行配置中删除了正确的用户，并且正确的用户仍保留在运行配置中：

a. 从历史记录窗格中选择 no user user2 password reallyhardpassword privilege 10 命令。

b. 点击 By Device 选项卡，然后点击 Execute a command on these devices。

c. 在命令窗格中，点击清除以清除命令窗格。

d. 输入命令 deploy memory，然后点击 Send。

查找所选 ASA 上的所有 SNMP 配置

此程序显示 ASA 运行配置中的所有 SNMP 配置条目。

步骤 1 在导航栏中，点击 **设备和服务**。

步骤 2 点击**设备 (Devices)** 选项卡以找到设备。

步骤 3 点击 **ASA** 选项卡。

步骤 4 过滤并搜索要在其上分析运行配置中的 SNMP 配置的设备，然后选择这些设备。

Note 确保您选择的设备已同步。设备未同步时，仅允许使用以下命令：show、ping、traceroute、vpn-sessiondb、changeto 和 dir。

步骤 5 在详细信息窗格中点击 **命令行接口 (Command Line Interface)**。您选择的设备位于我的列表窗格中。如果您决定将命令发送到更少的设备，请取消选中列表中的设备。

步骤 6 在命令窗格中，输入 show run | grep snmp，然后点击 Send。 运行配置文件中包含字符串 snmp 的所有行都将显示在响应窗格中。系统将打开“执行”选项卡，显示执行命令的设备。

步骤 7 查看响应窗格中的命令输出。

ASA 命令行接口文档

CDO 完全支持 ASA 命令行界面。我们在 CDO 中提供类似终端的接口，供用户同时向单个设备和多个设备发送 ASA 命令。ASA 命令行接口文档涵盖的范围非常广泛。这里不是在 CDO 文档中重新创建部分内容，而是指向 Cisco.com 上的 ASA CLI 文档。

ASA 命令行界面配置指南

从 ASA 9.1 版开始，《ASA CLI 配置指南》分为三本单独的指南：

- 《CLI 手册 1：思科 ASA 系列常规操作 CLI 配置指南》
- 《CLI 手册 2：思科 ASA 系列防火墙 CLI 配置指南》
- 《CLI 手册 3：思科 ASA 系列 VPN CLI 配置指南》

您可以通过以下方式访问 Cisco.com 上的 ASA CLI 配置指南：支持 (Support) > 按类别划分的产品 (Products by Category) > 安全 (Security) > 防火墙 (Firewalls) > ASA 5500 > 配置 (Configure) > 配置指南 (Configuration Guides)。

ASA 命令行界面配置指南的几个特定部分

过滤 show 和 more 命令输出。您可以在《CLI 手册 1：思科 ASA 系列常规操作 CLI 配置指南》的过滤 show 和 more 命令输出下了解如何使用正则表达式过滤 show 命令输出。

ASA 命令参考

《ASA 命令参考指南》按字母顺序列出了所有 ASA 命令及其选项。ASA 命令参考不是特定于版本的。它出版了四本书：

- 思科 ASA 系列命令参考，A - H 命令
- 思科 ASA 系列命令参考，I - R 命令
- 思科 ASA 系列命令参考，S 命令
- 思科 ASA 系列命令参考，适用于 ASASM 的 T - Z 命令和思科 IOS 命令

您可以通过以下方式访问 Cisco.com 上的《ASA 命令参考指南》：支持 (Support) > 按类别划分的产品 (Products by Category) > 安全 (Security) > 防火墙 (Firewalls) > ASA 5500 > 参考指南 (Reference Guides) > 命令参考 (Command References) > ASA 命令参考 (ASA Command References)。

导出 CDO CLI 命令结果

您可以将向独立设备或多个设备发出的CLI命令结果导出为逗号分隔值（.csv）文件，以便您可以随意过滤和排序其中的信息。您可以导出单个设备或多个设备的CLI结果。导出的信息包含以下内容：

- 设备
- 日期
- 用户
- 命令
- 输出

导出 CLI 命令结果

您可以将刚刚在命令窗口中执行的命令的结果导出到 .csv 文件：

步骤 1 在导航栏中，点击**设备和服务 (Devices & Services)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择一个或多个设备，使其突出显示。

步骤 5 在设备的**设备操作 (Device Actions)** 窗格中，点击**命令行接口 (Command Line Interface)**。

步骤 6 在命令行界面窗格中，输入命令并点击**发送 (Send)** 以向设备发出命令。

步骤 7 在已输入命令的窗口右侧，点击导出图标。

步骤 8 为 .csv 文件指定一个描述性名称，并将文件保存到本地文件系统。读取 .csv 文件上的命令输出时，展开所有单元格以查看命令的所有结果。

导出 CLI 宏的结果

您可以导出已在命令窗口中执行的宏的结果。使用以下程序可将在一台或多台设备上执行的 CLI 宏的结果导出到 .csv 文件：

步骤 1 打开 **设备和服务** 页面。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择一个或多个设备，使其突出显示。

步骤 5 在设备的**设备操作 (Device Actions)** 窗格中，点击**命令行接口 (Command Line Interface)**。

步骤 6 在 CLI 窗口的左侧窗格中，选择 CLI 宏收藏夹星型。

步骤 7 点击要导出的宏命令。填写任何适当的参数，然后点击发送。

步骤 8 在已输入命令的窗口右侧，点击导出图标 。

步骤 9 为 .csv 文件指定一个描述性名称，并将文件保存到本地文件系统。读取 .csv 文件上的命令输出时，展开所有单元格以查看命令的所有结果。

导出 CLI 命令历史记录

使用以下程序将一个或多个设备的 CLI 历史记录导出到 .csv 文件：

步骤 1 在导航窗格中，点击 **设备和服务**。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择一个或多个设备，使其突出显示。

步骤 5 在设备的“设备操作”(Device Actions) 窗格中，点击**命令行接口 (Command Line Interface)**。

步骤 6 如果历史记录窗格尚未展开，请点击时钟图标将其展开。

步骤 7 在已输入命令的窗口右侧，点击导出图标。

步骤 8 为 .csv 文件指定一个描述性名称，并将文件保存到本地文件系统。读取 .csv 文件上的命令输出时，展开所有单元格以查看命令的所有结果。

相关信息：

- CDO 命令行界面
- 创建 CLI 宏
- 删除 CLI 宏
- 编辑 CLI 宏
- 运行 CLI 宏
- ASA 批量 CLI 使用案例
- ASA 命令行接口文档
- 批量命令行接口

导出 CLI 宏列表

您只能导出已在命令窗口中执行的宏。使用以下程序将一个或多个设备的 CLI 宏导出到 .csv 文件：

步骤 1 在导航窗格中，点击 **设备和服务**。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择一个或多个设备，使其突出显示。

步骤 5 在设备的“设备操作”(Device Actions) 窗格中，点击**>_命令行接口 (>_Command Line Interface)**。

步骤 6 在 CLI 窗口的左侧窗格中，选择 CLI 宏收藏夹星型。

步骤 7 点击要导出的宏命令。填写任何适当的参数，然后点击发送。

步骤 8 在已输入命令的窗口右侧，点击导出图标。

步骤 9 为 .csv 文件指定一个描述性名称，并将文件保存到本地文件系统。

恢复 ASA 配置

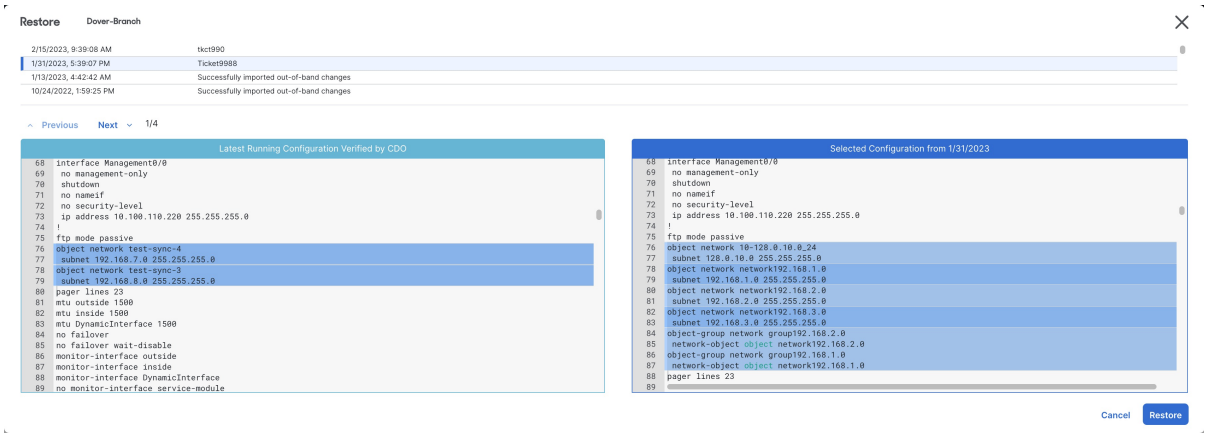
如果对 的配置进行了更改，并且想要恢复该更改，则可以恢复过去的配置。ASAASA这是一种删除具有意外或意外结果的配置更改的便捷方法。

关于恢复 ASA 配置

在恢复配置之前，请查看以下说明：

- 会将您选择要恢复的配置与部署到 的最后一个已知配置进行比较，但不会将您选择要恢复的配置与已暂存但未部署到 的配置进行比较。CDOASAASA如果您的上有任何未部署的更改，并且您恢复了过去的配置，则恢复过程将覆盖未部署的更改，您将丢失这些更改。ASA
- 在恢复过去的配置之前， 可以处于“已同步”或“未同步”状态，但如果设备处于“检测到冲突”状态，则必须先解决冲突，然后才能恢复过去的配置。ASA
- 恢复过去的配置会覆盖所有中间部署的配置更改。例如，从以下列表中的 1/31/2023 恢复配置会覆盖在 2/15/2023 所做的配置更改。
- 点击“Next”（下一步）和“Previous”（上一步）按钮将在配置文件中移动并突出显示配置文件更改
- 如果您最初对配置更改应用了更改请求标签，则该标签会显示在“恢复配置”列表中。

Figure 1: ASA 恢复配置屏幕



配置更改保留多长时间？

您可以恢复使用时间不超过 1 年的配置。恢复在其更改日志中记录的配置更改。ASACDO每次向 写入或读取配置更改时，更改日志都会记录更改。存储 1 年的变更日志，并且对上一年内进行的备份数量没有限制。ASACDO

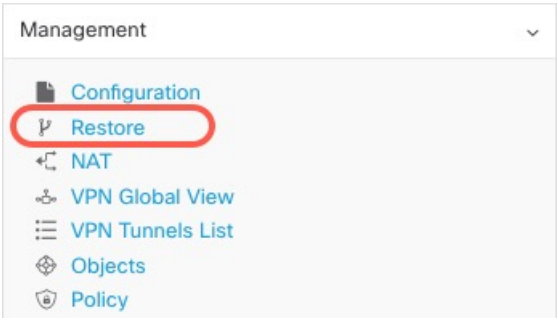
恢复 Secure Firewall ASA 配置

步骤 1 在导航栏中，点击**清单 (Inventory)**。

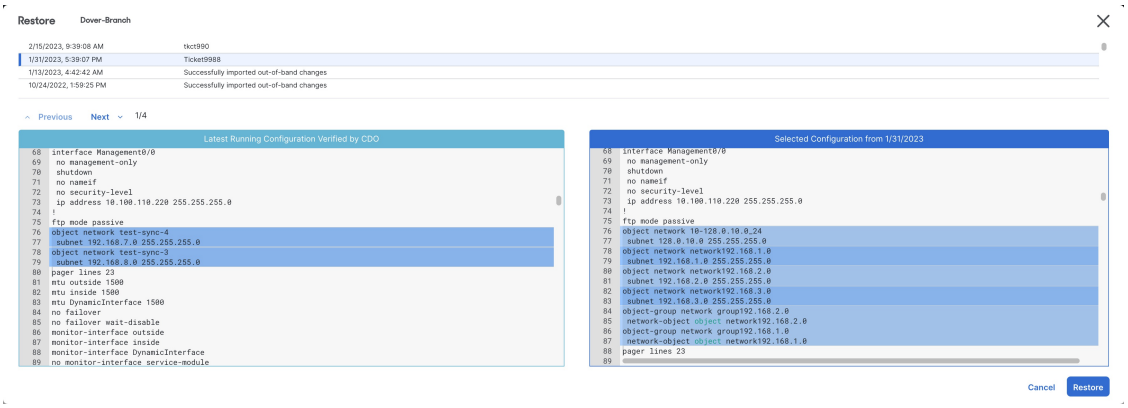
步骤 2 点击ASA选项卡。

步骤 3 选择您要恢复其配置的 ASA。

步骤 4 在**管理 (Management)** 窗格中，点击**恢复 (Restore)**。



步骤 5 在“恢复”(Restore) 页面中，选择要恢复的配置。



例如，在上图中，选择了 1/31/2023 的配置。

步骤 6 比较“由 CDO 验证的最新运行配置”和“自 < 日期 > 起的选定配置”，以确保您要恢复“自 < 日期 > 起的选定配置 > 窗口中显示的配置。使用“上一个”和“下一个”比较所有更改。

步骤 7 点击恢复，这将在 CDO 中暂存配置。在**清单 (Inventory)** 页面上，您会看到设备的配置状态现在为“未同步”(Not Synced)。

步骤 8 点击右侧窗格中的**部署更改...(Deploy Changes...)** 以部署更改并同步 ASA。

故障排除

如何恢复丢失但想要保留的更改？

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

步骤 3 点击 ASA 选项卡。

步骤 4 选择所需的设备。

步骤 5 点击右侧窗格中的更改日志。

步骤 6 查看更改日志中的更改。您可以根据这些记录重建丢失的配置。

管理 ASA 和 Cisco IOS 设备配置文件

某些类型的设备将其配置存储在单个文件中，例如 ASA 和 Cisco IOS 设备。对于这些设备，您可以在 Cisco Defense Orchestrator 上查看配置文件并在上面执行各种操作。

查看设备的配置文件

对于将整个配置存储在单个配置文件中的设备（例如 ASA、SSH 托管设备和运行Cisco IOS 的设备），您可以使用 CDO 查看配置文件。

注释 SSH 管理的设备和思科 IOS 设备具有只读配置。

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

步骤 3 点击设备类型选项卡。

步骤 4 选择要查看其配置的设备或型号。

步骤 5 在右侧的 **管理 (Management)** 窗格中，点击**配置 (Configuration)**。
系统将显示完整的配置文件。

相关信息：

- 编辑设备配置文件

编辑完整的设备配置文件

某些类型的设备将其配置存储在单个配置文件中，例如 ASA 。对于这些设备，您可以在 CDO 上查看设备配置文件，并根据设备对其执行各种操作。

目前，只能使用 CDO 直接编辑 ASA 配置文件。

Caution 此程序适用于熟悉设备配置文件语法的高级用户。此方法直接对 Defense Orchestrator 上存储的配置文件副本进行更改。

操作步骤

步骤 1 在导航栏中，点击**设备和服务 (Devices & Services)**。

步骤 2 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

步骤 3 点击 **ASA** 选项卡。

步骤 4 选择要编辑其配置的设备。

步骤 5 在右侧的 **管理 (Management)** 窗格中，点击**配置 (Configuration)**。

步骤 6 在设备配置页面中，点击编辑。

步骤 7 点击右侧的编辑器按钮，然后选择**默认**文本编辑器、**Vim** 或 **Emacs** 文本编辑器。

步骤 8 编辑文件并保存更改。

步骤 9 返回到设备和服务页面，预览并部署更改。

读取、丢弃、检查和部署更改

为了管理设备，CDO必须在其本地数据库中存储自己的设备配置副本。当CDO从其管理的设备“读取”配置时，它会获取设备配置的副本并将其保存。CDO首次在设备载入时读取并保存设备配置的副本。这些选项描述了出于不同目的而读取配置：

- 当设备的配置状态为“未同步”(Not Synced)时，可以使用**放弃更改 (Discard Changes)**。在“未同步”状态下，CDO上的设备配置有待更改。此选项允许您撤消所有待处理的更改。待处理的更改将被删除，并且 CDO 会使用设备上存储的配置副本覆盖其配置副本。
- **检查更改**。如果设备的配置状态为“已同步”(Synced)，则此操作可用。点击“检查更改”(Checking for Changes)会指示CDO将其设备配置副本与设备上存储的配置副本进行比较。如果存在差异，CDO 会立即使用设备上存储的副本覆盖其设备配置副本。
- **审核冲突**并**接受而不审核**。。如果您在设备上启用了冲突检测 (Conflict Detection)，CDO 会每10分钟检查一次设备上的配置更改。如果设备上存储的配置副本已更改，CDO会通过显示“检测到冲突“配置状态来通知您。
  - **查看冲突**。点击查看冲突，您可以查看直接在设备上进行的更改，并接受或拒绝这些更改。
  - **接受而不审核**。此操作会使用设备上存储的最新配置副本来覆盖设备配置的CDO副本。在执行覆盖操作之前，CDO 不会提示您确认配置的两个副本中的差异。

读取所有是一个批处理操作。您可以选择任何状态的多个设备，然后点击**读取全部 (Read All)**，以使用设备上存储的配置覆盖 CDO 上存储的所有设备的配置。

部署更改

当您更改设备的配置时，CDO会将您所做的更改保存到自己的配置副本中。在将这些更改部署到设备之前，这些更改在CDO上“待处理”。当设备的配置发生更改但尚未部署到设备时，该设备将处于“未同步”配置状态。

待处理的配置更改对通过设备运行的网络流量没有影响。只有在CDO将更改部署到设备后，它们才会生效。当CDO将更改部署到设备的配置时，它只会覆盖已更改的配置元素。它不会覆盖设备上存储的整个配置文件。可以为单个设备或同时在多个设备上启动部署。

注释 您可以安排部署或定期部署。有关详细信息，请参阅计划自动部署，第 166 页。

丢弃全部 (Discard All) 选项仅在您点击**预览并部署...(Preview and Deploy...)**。点击“预览并部署”(Preview and Deploy)后，CDO 会向您显示 CDO 中待处理更改的预览。点击**丢弃全部 (Discard All)** 会从CDO中删除所有待处理的更改，并且不会将任何内容部署到所选设备。与上面的“放弃更改”(Discard Changes)不同，删除待处理的更改是操作的结束。

读取所有设备配置

如果在 Cisco Defense Orchestrator (CDO) 之外对设备进行配置更改，则存储在 CDO 上的设备配置与其配置的本地副本将不再相同。您可能希望使用设备上存储的配置覆盖CDO的设备配置副本，以使配置再次相同。您可以使用**全部读取 (Read All)** 链接在多台设备上同时执行此任务。

有关 CDO 如何管理设备配置的两个副本的详细信息，请参阅读取、丢弃、检查和部署更改。

以下是三种配置状态，其中点击**全部读取 (Read All)** 将使用设备的配置副本覆盖 CDO 的设备配置副本。

- **检测到冲突 (Conflict Detected)** - 如果启用冲突检测，CDO 将每 10 分钟轮询一次其管理的设备，以了解对其配置所做的更改。如果 CDO 发现设备上的配置已更改，则 CDO 会显示设备的“检测到冲突”(Conflict detected) 配置状态。
- **已同步 (Synced)** - 如果设备处于同步状态，并且您点击**全部读取 (Read All)**，CDO 会立即检查设备以确定是否直接对其配置进行了任何更改。点击**读取全部 (Read All)** 后，CDO 会确认您是否打算覆盖其设备配置副本，然后 CDO 会执行覆盖。
- **未同步 (Not Synced)** - 如果设备处于未同步状态，并且您点击**全部读取 (Read All)**，则 CDO 会警告您使用CDO对设备的配置进行了待处理的更改，并且继续执行读取操作将删除这些更改，然后覆盖CDO 的配置副本以及设备上的配置。此读取所有功能，例如放弃更改。

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 （可选）创建更改请求标签以便在更改日志中轻松识别此批量操作的结果。

步骤 5 选择要保存 CDO 配置的设备。请注意，CDO 仅提供可应用于所有选定设备的操作的命令按钮。

步骤 6 点击**全部读取 (Read All)**。

步骤 7 如果您选择的任何设备的 CDO 上有配置更改，CDO 会发出警告，并询问您是否要继续执行批量读取配置操作。点击**全部读取 (Read All)** 以继续。

步骤 8 查看通知选项卡以了解“全部读取”(Read All) 配置操作的进度。如果您想了解有关批量操作中各个操作是如何成功或失败的更多信息，请点击蓝色查看链接，您将被定向到“作业”(Jobs) 页面。

步骤 9 如果您创建并激活了更改请求标签，请记住将其清除，以免无意中将其他配置更改与此事件关联。

相关信息

- 读取、丢弃、检查和部署更改
- 放弃更改
- 检查配置更改

将 ASA 的配置更改读取到 CDO

为什么 Cisco Defense Orchestrator 会“读取”ASA 配置？

为了管理 ASA，CDO 必须拥有自己存储的 ASA 运行配置文件副本。CDO 首次读取并保存设备配置文件的副本是在设备载入时。随后，当 CDO 从 ASA 读取配置时，您将选择**检查更改 (Check for Changes)**、**接受而不审核 (Accept without Review)** 或**读取配置 (Read Configuration)**。有关详细信息，请参阅读取、丢弃、检查和部署更改。

在以下情况下，CDO 还需要读取 ASA 配置：

- 将配置更改部署到 ASA 失败，并且设备状态未列出或**未同步 (Not Synced)**。
- 载入设备失败，设备状态为“未配置”。
- 您已在 CDO 之外对设备配置进行了更改，但尚未轮询或检测到这些更改。设备状态为“已同步”或“已检测到冲突”。

在这些情况下，CDO 需要存储在设备上的最后一个已知配置的副本。

读取 ASA 上的配置更改

当系统提示读取 ASA 上的配置更改时：

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择 CDO 最近未能载入的设备或 CDO 未能将更改部署到的设备。

步骤 5 点击右侧“已同步”窗格中的**读取配置**。此选项会覆盖当前保存到 CDO 的配置。

预览和部署所有设备的配置更改

当您对租户上的设备进行了配置更改，但您尚未部署该更改时，CDO 会通过在部署图标上显示一个橙色点来通知您

。受这些更改影响的设备在设备和**服务 (Services)** 页面中显示“未同步”(Not Synced) 状态。通过点击**部署 (Deploy)**，您可以查看哪些设备具有待处理的更改，并将更改部署到这些设备。

注释 对于您创建和更改的每个新 FDM 或 FTD 网络对象或组，CDO 会在此页面中为 CDO 管理的所有 本地管理中心 创建一个条目。

此部署方法适用于所有受支持的设备。

您可以将此部署方法用于单个配置更改，也可以等待并一次部署多个更改。

步骤 1 在屏幕的右上角，点击**部署 (Deploy)** 图标 。

步骤 2 选择要部署更改的设备。如果设备有黄色警告三角形，则无法将更改部署到该设备。将鼠标悬停在黄色警告三角形上，了解无法将更改部署到该设备的原因。

步骤 3 （可选）如果要查看有关待处理更改的更多信息，请点击**查看详细更改日志 (View Detailed Changelog)** 链接以打开与该更改关联的更改日志。点击**部署 (Deploy)** 图标可返回**具有待处理更改的设备 (Devices with Pending Changes)** 页面。

步骤 4 （可选）创建更改请求以跟踪更改，而无需离开**具有待处理更改的设备 (Devices with Pending Changes)** 页面。

步骤 5 点击**立即部署 (Deploy Now)**，立即将更改部署到您选择的设备。您将在“作业”(Jobs) 托盘的“活动作业”(Active jobs) 指示器中看到进度。

步骤 6 （可选）部署完成后，点击 CDO 导航栏中的**作业 (Jobs)**。您将看到最近的“部署更改”(Deploy Changes) 作业，其中显示了部署的结果。

步骤 7 如果您创建了更改请求标签，并且没有其他配置更改与之关联，请将其清除。

下一步做什么

- 已计划的自动部署
- 将配置更改从 CDO 部署到 ASA，第 161 页
- 部署到 ASA 后的更改日志条目

将配置更改从 CDO 部署到 ASA

为什么 CDO 会将更改部署到 ASA？

当您使用 Cisco Defense Orchestrator (CDO) 管理和更改设备配置时，CDO 会将您所做的更改保存到自己的配置文件副本中。在“部署”到设备之前，这些更改将被视为已在 CDO 上“暂存”。暂存配置更改对通过设备运行的网络流量没有影响。只有在 CDO 将更改“部署”到设备后，它们才会影响通过设备运行的流量。当 CDO 将更改部署到设备的配置时，它只会覆盖已更改的配置元素。它不会覆盖设备上存储的整个配置文件。

ASA 有一个“运行”的配置文件（有时称为“运行配置”）和一个“启动”配置文件（有时称为“启动配置”）。对通过 ASA 的流量会强制执行运行配置文件中存储的配置。对运行配置进行更改

并对这些更改产生的行为感到满意后，您可以将其部署到启动配置。如果ASA重新启动，它会使用启动配置作为其配置起点。重新启动ASA后，您对运行配置所做的任何未保存到启动配置的更改都将丢失。

在将更改从 CDO 部署到 ASA 时，这些更改会被写入运行配置文件。在对这些更改产生的行为感到满意后，您就可以将这些更改部署到启动配置文件。

部署可以为单个设备或同时在多个设备上启动。您可以为单个设备安排单独的部署或定期部署。

某些更改会被直接部署到 ASA

如果您在 CDO 上使用 CLI 接口 CLI 宏接口来对 ASA 进行更改，则这些更改不会被“暂存”在 CDO 上。它们会被直接部署到 ASA 的运行配置中。在以这种方式进行更改时，您的设备会与 CDO 保持“同步”。

关于部署配置更改

本部分假定您使用 CDO 的 GUI 或编辑“设备配置”页面，而不是使用 CDO 的 CLI 界面或 CLI 宏界面对 ASA 配置文件进行更改。

更新 ASA 配置的过程分为两步。

步骤 1 使用以下方法之一对 CDO 进行更改：

- CDO GUI
- “设备配置”页面上的设备配置

步骤 2 进行更改后，返回到**清单 (Inventory)** 页面，然后选择**预览并部署... (Preview and Deploy...)**以预览并部署更改到设备。

下一步做什么

当 CDO 使用暂存在 CDO 上的运行配置更新 ASA 的运行配置时，或者当它使用存储在 ASA 上的运行配置更改CDO上的配置时，它会尝试仅更改配置文件的相关行，前提是配置的该方面可以由CDO GUI 管理。如果无法使用 CDO GUI 进行所需的配置更改，CDO 会尝试覆盖整个配置文件以进行更改。

以下是两个示例：

- 您可以使用 CDO GUI 创建或更改网络对象。如果 CDO 需要将该更改部署到 ASA 的配置，则会在发生更改时覆盖 ASA 上正在运行的配置文件的相关行。
- 您**无法**使用 CDO GUI 创建新的本地 ASA 用户，但可以通过编辑“设备配置”(Device Configuration) 页面上的ASA配置来创建本地用户。如果您在“设备配置”页面上添加用户，并将该更改部署到 ASA，CDO 将通过覆盖整个运行配置文件来尝试将该更改保存到 ASA 的运行配置文件。

部署使用 CDO GUI 进行的配置更改

步骤 1 在使用 CDO GUI 进行配置更改并保存更改后，该更改将保存在 ASA 的运行配置文件的 CDO 存储版本中。

步骤 2 返回**清单 (Inventory)** 页面上的设备。

步骤 3 点击设备选项卡。您应该会看到设备现在处于“未同步”(Not synced) 状态。

步骤 4 使用以下方法之一部署更改：

- 点击屏幕右上角的**部署 (Deploy)** 图标  。这使您有机会在部署之前查看对设备进行的更改。检查您所做更改的设备，展开设备以查看更改，点击**立即部署 (Deploy Now)** 以部署更改。

  注释 如果在“有待处理更改的设备”(Devices with Pending Changes) 屏幕上看到设备旁边显示黄色警告三角形，则无法部署更改。将鼠标悬停在警告三角形上，了解无法将更改部署到设备的原因。

- 在未同步窗格中，点击**预览并部署... (Preview and Deploy...)**。

  1. 查看将更改 ASA 配置文件的命令。
  2. 如果您对命令感到满意，请选择“配置恢复首选项”(Configuration Recovery Preference)。

     注释 如果您选择“告诉我，我将手动恢复配置”(Let me know and I will restore the configuration manually)，请在继续之前点击**查看手动同步说明 (View Manual Synchronization Instructions)**。

  3. 点击**将更改应用到设备 (Apply Changes to Device)**。
  4. 点击成功消息中的**确定 (OK)**。

计划自动部署

您还可以配置租户，通过计划自动部署来将部署安排到具有待定更改的单个设备或所有设备。

使用 CDO 的 CLI 界面部署配置更改

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择要更改其配置的设备。

步骤 5 在**操作 (Actions)** 窗格中，点击**>_命令行接口 (>_Command Line Interface)**。

步骤 6 如果命令行界面表中有任何命令，请点击清除以将其删除。

步骤 7 在命令行界面表的顶部框中，在命令提示符下输入命令。您可以运行单个命令，也可以通过在其自己的行中输入每个命令或输入配置文件的一部分作为命令来运行批处理中的多个命令。以下是您可以在命令行界面表中输入的一些命令示例：

创建网络对象“albany”的单个命令

```
object network albany
host 209.165.30.2
```

多个命令一起发送：

```
object network albany
host 209.165.30.2
object network boston
host 209.165.40.2
object network cambridge
host 209.165.50.2
```

作为命令输入的运行配置文件的一部分：

```
interface GigabitEthernet0/5
 nameif guest
 security-level 0
 no ip address
```

注释 CDO 不要求您在 EXEC 模式、特权 EXEC 模式和全局配置模式之间切换。它会解释您在适当的上下文中输入的命令。

步骤 8 输入命令后，点击发送。在 CDO 成功部署对 ASA 的运行配置文件的更改后，您会收到消息“完成！”(Done!)。

步骤 9 发送命令后，您可能会看到消息“某些命令可能已对运行配置进行了更改”(Some commands may have made changes to the running config) 以及两个链接。

- 点击**部署到磁盘 (Deploy to Disk)** 会将此命令所做的更改以及运行配置中的任何其他更改保存到 ASA 的启动配置中。
- 点击**消除 (Dismiss)**，可关闭消息。

通过编辑设备配置部署配置更改

⚠

注意 此程序适用于熟悉ASA配置文件语法的高级用户。此方法直接更改存储在CDO上的运行配置文件。

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择要更改其配置的设备。

步骤 5 点击操作窗格中的查看配置。

步骤 6 点击**编辑**。

步骤 7 对运行配置进行更改并保存。

步骤 8 返回**清单 (Inventory)** 页面。在未同步窗格中，点击**预览并部署... (Preview and Deploy...)**。

步骤 9 在设备同步窗格中，查看更改。

步骤 10 根据更改的类型，点击替换配置或将更改应用到设备。

在多个设备上部署共享对象的配置更改

对两台或多台设备共享的策略或对象进行更改时，请使用此程序。您可以在许多设备上更改通用策略。

步骤 1 打开并编辑包含要编辑的共享对象的策略页面或对象页面。

步骤 2 查看共享设备列表，并确认要对提及的所有设备进行更改。

步骤 3 点击 **Confirm**。

步骤 4 点击**保存 (Save)**。

步骤 5 点击**部署**图标 并预览和部署所有设备的配置更改。

批量部署设备配置

如果您对多个设备进行了更改（例如通过编辑共享对象），则可以一次将这些更改应用到所有受影响的设备：

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择已在 CDO 上进行配置更改的所有设备。这些设备应显示“未同步”(Not Synced) 状态。

步骤 5 使用以下方法之一部署更改：

- 点击屏幕右上角的 按钮可查看**有待处理更改的设备 (Devices with Pending Changes)** 窗口。这使您有机会在部署之前查看所选设备上的待处理更改。点击**立即部署 (Deploy Now)** 以部署更改。

  Note 如果在**有待处理更改的设备 (Devices with Pending Changes)** 屏幕上看到某个设备旁边显示黄色警告三角形，则无法将更改部署到该设备。将鼠标悬停在警告三角形上，了解有关无法将更改部署到该设备的信息。

- 点击详细信息窗格中的**全部部署 (Deploy All)** 。查看所有警告，然后点击**确定 (OK)**。批量部署会立即开始，无需审核更改。

步骤 6 （可选）点击导航栏中的“作业”(Jobs) 图标  以查看批量部署的结果。

相关信息：

- 计划自动部署, on page 166

已计划的自动部署

通过使用CDO，您可以对其管理的一个或多个设备进行配置更改，然后安排在您方便的时间将更改部署到这些设备。

只有您在“设置”(Settings) 页面的**租户设置 (Tenant Settings)** 选项卡中 启用计划自动部署的选项 才能安排部署。一旦启用此选项，您就可以创建、编辑或删除计划部署。计划的部署会在设置的日期和时间部署在 CDO 上保存的所有暂存更改。您还可以在“作业”(Jobs) 页面中查看和删除计划部署。

如果直接对设备进行了尚未读取、丢弃、检查和部署更改到CDO的更改，则将跳过计划的部署，直到该冲突得以解决。“作业”(Jobs)页面将列出计划部署失败的所有实例。如果**启用计划自动部署的选项 (Enable the Option to Schedule Automatic Deployments)** 被关闭，则所有计划的部署都将被删除。

Caution 如果您为多台设备安排新的部署，并且其中一些设备已安排了部署，则新的安排部署将覆盖现有的安排部署。

Note 当您创建计划部署时，将按照本地时间来创建计划，而不是设备的时区。计划的部署不会自动调整夏令时。

计划自动部署

部署计划可以是单个事件或周期性事件。您可能会发现定期自动部署是一种将定期部署与维护窗口对齐的便捷方式。请按照以下程序为单个设备安排一次性或周期性部署：

Note 如果为已安排现有部署的设备安排部署，新的安排部署将覆盖现有部署。

步骤 1 在导航栏中，点击 **设备和服务**。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择一个或多个设备。

步骤 5 在设备详细信息窗格中，找到计划的部署选项卡，然后点击**计划 (Schedule)**。

步骤 6 选择应进行部署的时间。

- 对于一次性部署，请点击**一旦开启 (Once on)** 选项以从日历中选择日期和时间。
- 对于周期性部署，请点击**每次 (Every)** 选项。您可以选择每天或每周一次部署。选择部署的**日期 (Day)** 和**时间 (Time)**。

步骤 7 点击**保存 (Save)**。

编辑计划部署

请按照以下程序编辑计划部署：

步骤 1 在导航栏中，点击 **设备和服务**。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择一个或多个设备。

步骤 5 在**设备详细信息 (Device Details)** 窗格中，找到计划的部署选项卡，然后点击**编辑 (Edit)**。

步骤 6 编辑计划部署的重复周期、日期或时间。

步骤 7 点击**保存 (Save)**。

删除计划部署

请按照以下程序删除计划部署：

Note 如果为多台设备安排部署，然后更改或删除某些设备的安排，则其余设备的原始安排部署将保留。

步骤 1 在导航栏中，点击**设备和服务 (Devices & Services)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择一个或多个设备。

步骤 5 在**设备详细信息 (Device Details)** 窗格中，找到计划的部署选项卡，然后点击**删除 (Delete)** 。

What to do next

- 读取、丢弃、检查和部署更改
- 读取所有设备配置, on page 159
- 将配置更改从 CDO 部署到 ASA, on page 161
- 预览和部署所有设备的配置更改, on page 160

检查配置更改

检查更改以确定设备的配置是否已直接在设备上更改，并且它不再与CDO上存储的配置副本相同。当设备处于“已同步”(Synced) 状态时，您将看到此选项。

要检查更改，请执行以下操作：

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择您怀疑其配置可能已直接在设备上更改的设备。

步骤 5 点击右侧“已同步”(Synced) 窗格中的**检查更改 (Check for Changes)**。

步骤 6 以下行为因设备而有细微差别：

- 对于 设备，如果设备的配置发生变化，您将收到以下消息：

  从设备读取策略。如果设备上有活动的部署，则将在完成后开始读取。

  - 点击 **OK** 继续操作。设备上的配置将覆盖 CDO 上存储的配置。
  - 点击**取消 (Cancel)** 以取消操作。

- 对于 ASA 设备：

a. 比较呈现给您的两种配置。点击**继续**。标记为**最后已知的设备配置 (Last Known Device Configuration)** 的配置是存储在 CDO 上的配置。标记为 **在设备上找到 (Found on Device)** 的配置是保存在 ASA上的配置。

b. 选择以下选项中的一种：

1. **拒绝**带外更改以保留“最后已知的设备配置”(Last Known Device Configuration)。
2. **接受**带外更改，以使用设备上找到的配置来覆盖 CDO 中存储的设备配置。

c. 点击**继续**。

放弃更改

如果要“撤消”使用 CDO 对设备配置所做的所有未部署的配置更改，请点击**放弃更改 (Discard Changes)**。在点击**放弃更改 (Discard Changes)** 时，CDO 会使用设备上存储的配置完全覆盖设备配置的本地副本。

点击**放弃更改 (Discard Changes)** 时，设备的配置状态为**未同步 (Not Synced)**。在放弃更改后，CDO 上的配置副本将与设备上的配置副本相同，CDO 中的配置状态将恢复为“已同步”(Synced)。

要放弃或“撤消”设备的所有未部署的配置更改，请执行以下操作：

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择您已对其进行配置更改的设备。

步骤 5 点击右侧**未同步 (Not Synced)** 窗格中的**放弃更改 (Discard Changes)**。

- 对于 FDM 管理 设备，CDO 会警告您“CDO 上的待处理更改将被丢弃，此设备的 CDO 配置将替换为设备上当前运行的配置”(Pending changes on CDO will be discarded and the CDO configuration for this device will be replaced with the configuration currently running on the device)。点击**继续 (Continue)** 以放弃更改。
- 对于 Meraki 设备 - CDO 会立即删除更改。
- 对于 AWS 设备 - CDO 会显示您要删除的内容。点击**接受 (Accept)** 或**取消 (Cancel)**。

设备上的带外更改

带外更改是指在不使用 CDO 的情况下直接在设备上进行的更改。这些更改可以通过 SSH 连接使用设备的命令行界面，或使用本地管理器（如适用于 ASA 的自适应安全设备管理器 (ASDM)、适用于 FDM 管理 管理设备的 FDM 或 本地防火墙管理中心 用户界面上的 本地防火墙管理中心）来进行。带外更改会导致 CDO 上存储的设备配置与设备本身上存储的配置之间发生冲突。

检测设备上的带外更改

如果为 ASA、FDM 管理 设备、Cisco IOS 设备或 本地防火墙管理中心 启用了冲突检测，则 CDO 会每 10 分钟检查一次设备，以搜索在 CDO 之外直接对设备配置进行的任何新更改。

如果 CDO 发现未存储在 CDO 上的设备配置更改，则会将该设备的**配置状态**更改为“检测到冲突”状态。

当 Defense Orchestrator 检测到冲突时，可能出现以下两种情况：

- 直接对设备进行的配置更改尚未保存到 CDO 的数据库中。
- 对于 FDM 管理 设备，FDM 管理 设备上可能存在尚未部署的“待处理”配置更改。
- 对于 本地防火墙管理中心，可能会对 CDO 外部的对象进行更改，而这些更改会等待与 CDO 同步，或者在 CDO 中进行的更改等待部署到 本地防火墙管理中心。

同步 Defense Orchestrator 和设备之间的配置

关于配置冲突

在**清单 (Inventory)** 页面上，您可能会看到设备或服务的状态为“已同步”(Synced)、“未同步”(Not Synced) 或“检测到冲突”(Conflict Detected)。要了解使用 CDO 管理的 本地防火墙管理中心 的状态，请导航至**工具和服务 (Tools & Services)** > **防火墙管理中心 (Firewall Management Center)**。

- 如果设备为**已同步 (Synced)**， Cisco Defense Orchestrator (CDO) 上的配置与设备本地存储的配置相同。
- 如果设备为**未同步 (Not Synced)**，CDO 中存储的配置已更改，现在存储在设备上的配置有所不同。将您的更改从 CDO 部署到设备会更改设备上的配置以匹配 CDO 的版本。
- 在CDO之外对设备进行的更改称为**带外更改**。进行带外更改时，如果为设备启用了冲突检测，您会看到设备状态更改为“检测到冲突”(Conflict Detected)。接受带外更改会更改 CDO 上的配置以匹配设备上的配置。

冲突检测

启用冲突检测后， Cisco Defense Orchestrator (CDO) 将按默认间隔轮询设备，以确定是否在 CDO 之外对设备配置进行了更改。如果CDO检测到已进行更改，则会将设备的配置状态更改为**检测到冲突 (Conflict Detected)**。在 CDO 之外对设备进行的更改称为“带外”更改。

对于由 CDO 管理的 本地防火墙管理中心 ，如果存在已暂存的更改且设备处于**未同步 (Not Synced)** 状态，则CDO会停止轮询设备以检查更改。当在CDO外部进行的更改等待与CDO同步，而在CDO中进行的更改等待部署到 本地管理中心 时，CDO 会声明 本地管理中心 处于**检测到冲突 (Conflict Detected)** 状态。

启用此选项后，您可以配置每台设备检测冲突或OOB更改的频率。有关详细信息，请参阅安排设备更改轮询, on page 173。

启用冲突检测

启用冲突检测会提醒您在 Defense Orchestrator 之外对设备进行更改。

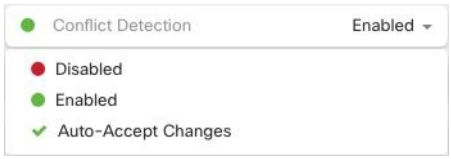
步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备**选项卡。

步骤 3 选择适当的设备类型选项卡。

步骤 4 选择要启用冲突检测的设备。

步骤 5 在设备表右侧的冲突检测框中，从列表中选择已启用。



自动接受设备的带外更改

您可以通过启用自动接受更改，将 Cisco Defense Orchestrator (CDO) 配置为自动接受直接对受管设备所做的任何更改。不使用 CDO 直接对设备进行的更改称为带外更改。带外更改会在 CDO 上存储的设备配置与设备本身上存储的配置之间产生冲突。

自动接受更改功能是对冲突检测的增强。如果您在设备上启用了自动接受更改，CDO 会每 10 分钟检查一次更改，以确定是否对设备的配置进行了任何带外更改。如果配置发生更改，CDO 会自动更新其本地版本的设备配置，而不会提示您。

如果对 CDO 进行的配置更改尚未部署到设备，则 CDO **不**会自动接受配置更改。按照屏幕上的提示确定下一步操作。

要使用自动接受更改，请先启用租户，以在**清单 (Inventory)** 页面中显示自动接受选项；然后，您可以为单个设备启用自动接受更改。

如果您希望 CDO 检测带外更改，但为您提供手动接受或拒绝更改的选项，请改为启用 冲突检测, on page 170。

配置自动接受更改

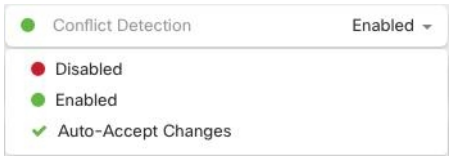
步骤 1 使用具有管理员或超级管理员权限的帐户登录 CDO。

步骤 2 从 CDO 菜单中，导航至 **设置 (Settings)** > **常规设置 (General Settings)**。

步骤 3 在租户设置区域中，点击切换按钮以启用“自动接受设备更改的选项”。这将使“自动接受更改”菜单选项显示在**清单 (Inventory)** 页面的“冲突检测”菜单中。

步骤 4 打开**清单 (Inventory)** 页面，然后选择要自动接受带外更改的设备。

步骤 5 在“冲突检测”(Conflict Detection) 菜单中，选择下拉菜单中的“自动接受更改”(Auto-Accept Changes)。



为租户上的所有设备禁用自动接受更改

步骤 1 使用具有管理员或超级管理员权限的帐户登录 CDO。

步骤 2 从 CDO 菜单中，导航至 **设置 (Settings)** > **常规设置 (General Settings)**

步骤 3 在“租户设置”区域中，通过将切换开关向左滑动来禁用“启用自动接受设备更改的选项”，使其显示灰色 X。这将禁用“冲突检测”菜单中的“自动接受更改”选项，并为以下项禁用此功能：租户上的每台设备。

Note 禁用“自动接受”将要求您查看每个设备冲突，然后才能将其接受到CDO中。这包括之前配置为自动接受更改的设备。

解决配置冲突

本节提供有关解决设备上发生的配置冲突的信息。

解决“未同步”状态

使用以下程序解决配置状态为“未同步”的设备：

步骤 1 在导航栏中，点击**清单 (Inventory)**。

Note 对于 本地防火墙管理中心，请导航至**工具和服务 (Tools & Services)** > **防火墙管理中心 (Firewall Management Center)** 并选择处于**未同步 (Not Synced)** 状态的 FMC，然后从步骤 5 继续操作。

步骤 2 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

步骤 3 点击设备类型选项卡。

步骤 4 选择报告为“未同步”的设备。

步骤 5 在右侧的未同步面板中，选择以下任一选项：

- **预览并部署...** - 如果要将配置更改从 CDO 推送到设备，请预览并部署您现在所做的更改，或者等待并一次部署多个更改。预览和部署所有设备的配置更改, on page 160

- 放弃更改 - 如果您不想将配置更改从 CDO 推送到设备，或者您想要“撤消”您开始在 CDO 上进行的配置更改。此选项使用设备上存储的运行配置覆盖 CDO 中存储的配置。

解决“检测到冲突”状态

CDO 允许您在每个实时设备上启用或禁用冲突检测。如果 冲突检测, on page 170 已启用，并且在未使用 CDO 的情况下对设备的配置进行了更改，则设备的配置状态将显示为**检测到冲突 (Conflict Detected)**。

要解决“检测到冲突”(Conflict Detected) 状态，请执行以下程序：

步骤 1 在导航栏中，点击**清单 (Inventory)**。

Note 对于 本地防火墙管理中心，请导航至**工具和服务 (Tools & Services)** > **防火墙管理中心 (Firewall Management Center)** 并选择处于**检测到冲突 (Conflict Detected)** 状态的 FMC，然后从步骤 4 继续操作。

步骤 2 点击**设备 (Devices)** 选项卡以找到设备。

步骤 3 点击设备类型选项卡。

步骤 4 选择报告冲突的设备，然后点击右侧详细信息窗格中的**查看冲突 (Review Conflict)**。

步骤 5 在**设备同步 (Device Sync)** 页面中，通过查看突出显示的差异来比较两种配置。

- 标记为“最后一次设备配置”(Last Known Device Configuration) 的面板是存储在 CDO 上的设备配置。
- 标记为“在设备上找到”(Found on Device) 的面板是存储在运行 ASA 配置中的配置。

步骤 6 通过选择以下选项之一来解决冲突：

- **接受设备更改 (Accept Device changes)**：这将使用设备的运行配置覆盖 CDO **上存储的配置** 和任何待处理的更改。

  Note 由于 CDO 不支持在命令行界面之外部署对Cisco IOS 设备的更改，因此在解决冲突时，您对Cisco IOS 设备的唯一选择是选择**接受而不查看 (Accept Without Review)**。

- **拒绝设备更改 (Reject Device Changes)**：这将使用存储在 CDO 上的配置覆盖设备上存储的配置。

Note 所有配置更改（拒绝或接受）都记录在更改日志中。

安排设备更改轮询

如果已启用 冲突检测, on page 170 或从“设置”(Settings) 页面 **启用自动接受设备更改的选项 (Enable the option to auto-accept device changes)**，则 CDO 将按默认间隔轮询设备，以确定是否在 CDO 之

外对设备配置进行了更改。您可以自定义CDO轮询每台设备更改的频率。这些更改可以应用于多个设备。

如果没有为设备配置选择，则会自动为“租户默认”配置间隔。

Note 从**设备和服务 (Devices & Services)** 页面自定义每台设备的间隔会覆盖从**常规设置 (General Settings)** 页面选择作为默认冲突检测间隔 (Default Conflict Detection Interval) 的轮询间隔。

从**设备和服务 (Devices & Services)** 页面启用**冲突检测 (Conflict Detection)** 或从“设置”(Settings) 页面选择**启用该选项以自动接受设备更改 (Enable the option to auto-accept device changes)** 后，请使用以下程序来安排您希望 CDO 轮询设备的频率：

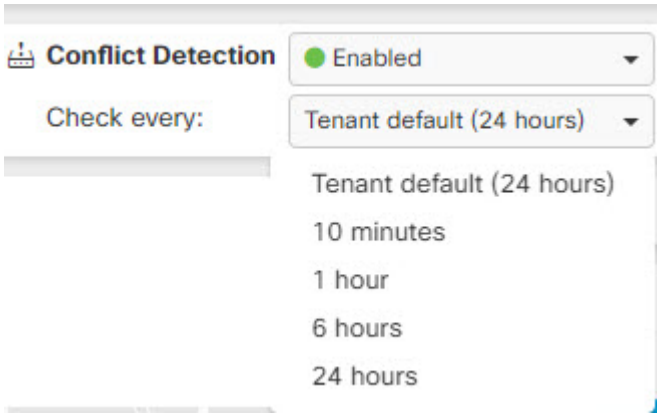
步骤 1 在导航栏中，点击 **设备和服务**。

步骤 2 点击 **设备** 选项卡，找到您的设备。

步骤 3 点击设备类型选项卡。

步骤 4 选择要启用冲突检测的设备。

步骤 5 在与**冲突检测 (Conflict Detection)** 相同的区域中，点击**检查间隔 (Check every)** 下拉菜单，然后选择所需的轮询间隔：



当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。